CCNA

Introduction

[1] Network definition

[2] Network components :-
* HTTP * FTP * SMTP * pop3 * Telnet

[4] Network topologies
* P-P * Star * Bus * Mesh * Ring

[5] Network types
* LAN * WAN * MAN

[8] OSI Model

[12] TCP/IP Model

[13] Typical Network Components
* PC * Hub * switch * Router * Modem

[15] DTE & DCE

[16] physical layer
* LAN Cables

[18] LAN standards & Twisted pair Categories

[19] LAN Connectors
* Straight & cross & consol cables

[23] Data link layer
* MAC address
* types of dst MAC ↔ unicast, Broadcast, Multicast

[25] MAC Method
* CSMA/CD

[26] MAC Flow Control
* Buffering * congestion avoidance
- MAC Frame

[28] layer 2 devices
* NIC * Bridge * switch

[29] Switch operation
* learning

[30] Forwarding
* Flood If Dst MAC ↔ unkown unicast, Multicast, Broadcast

[31] Microsegmentation
* to avoid Collision in switch

[32] switch Forwarding Modes (types)
* cut through * Fragment Free
* store & forward * adaptive cut through

[33] Remove L2 loops (STP)

[34] L3 : internet layer

[35] Router operation
* learning * forwarding

[36] IP V4
* TOS * TTL

[37] ICMP (internet control Messaging protocol)
→ * ping www.facebook.com
→ * Trace www.facebook.com

[38] IPV4 Classes
- Class A, B, C, D, E
- Classless IPs

[41] NAT

[42] subnetting

[45] Getting started for end to end data delivery
-src ip Manually

[46] - automatically [DHCP]

[47] - dst ip

[48] dst MAC [ARP] address resolution protocol

[50] L4 : transport layer
- Port no & socket no

[51] TCP & UDP in L4

[53] Old subnetting standard

Routing

[54] Routing introduction
- Routed & Routing protocol
- static & dynamic Routing

[55] Autonomous sys.

[56] admis. distance - metric

[57] Static routing → RIP v1

[58] Distance vector [RIP v1]

[59] . at start up

[60] at convergance , at change

[62] Triggered update + poison rout & reverse

[63] split horizon

64 Hold down timer

65 RIPv1 & IGRP c/c's

66 Advanced D.V
* Rip V_2

67 EIGRP
* Start up

69 at convergance

70 at change

72 EIGRP c/c's

73 Link State
* ospf * Start up

75 -at change
-at convergence
- ospf c/c's

76 Hirarchical design

78 Route summarization and CIDR
(supper networking)

80 ospf operation in multiple access
* Router ID

81 neighor discovery

82 Routes discovery
* Electing of DR & BDR

83 VLSM [Veriable length Subnet Mask]

84 NAT
* static * dynamic

85 PAT

switching

86 STP (at start up)
* BPDU Flooding * Electing root switch and root port

89 Electing Disegnated port
* Blocked port

91 at change
* direct & indirect change

92 RSTP

94 VLAN
* Inter VLAN Routing

* Traditional solutions
* Router on a stick
* Multilayer switch

96 switch port types
* access * Trunk

97 Tagged types
* ISL * IEEE802.1q

98 VLAN Configuration

99 static & Dynamic VLAN membership

100 DTP

100 Managing switch remotely

101 VTP
* VTP operation

104 wi Fi

105 wifi standards
IEEE 802.11 b/G/n/A

106 wifi design
* ad hoc * infrastructure mode

108 WAN switching

108 * circuit switching

109 * packet ~

110 * Broadband Technology

111 DSL
* ADSL * SDSL

111 Cis protocols
* encapsulation
* HDLC * PPP
* configuration

113 PPP operation
* LCP * NCP

114 PPP Negotiation
- error correction - Compression
- Multilink - Call Back
- Authentication

115 PAP - CHAP authentic

116 CSU/DSU Digital Modem

117 Packet switching (FR)
- FR Encapsulation

118 FR operation
- LMI - IARP

120 FR issue & solutions

122 Security
- types of attaks

125 switch security

126 Router ~
- ACL types

127 IP Standard ACL
- create ACL

128 - activate ACL & Examples

130 IP Extended ACL
- Create ACL

131 activate ACL & EX

132 firewall

134 IDS & IPS

135 VPN

136 -VPN devices & protocols
- VPN operation ⇄ C I A

139 security types
- PSK - WPA - WPA2

140 IPV6

143 NDP

144 IPV6 types (addressing)

145 APIPA

146 IPV6 end to end data delivery
* MPLS * MobileIP

147 IPV4 to IPV6 translation
* Dual Stack * NAT-PT
* Tunneling

149 How to recover password

a N1 lazy

Network definition / it is a group of components that are connected together to provide a service ← application

Mobile Network
Telephony ~] → they are not our course

⇒ our course is about data network (IP Network)

Network Importance

① Easy sharing of files, information and data

② Easy sharing of Expinsive resources (devices)

③ Modern live
- voice over IP
- vedio conference
- Telepresense
- smell
- touch
- Games (as call of duty)
- life

Network components

[1] Computer / it is the main component, because it is the soure of Network application

↳ services that can be done with a remote device

operating systems
- windows
- Linux
- Unix
- Mac OS
- android ⟶ OS for Mobile
- ios ⟶ OS for apple devices

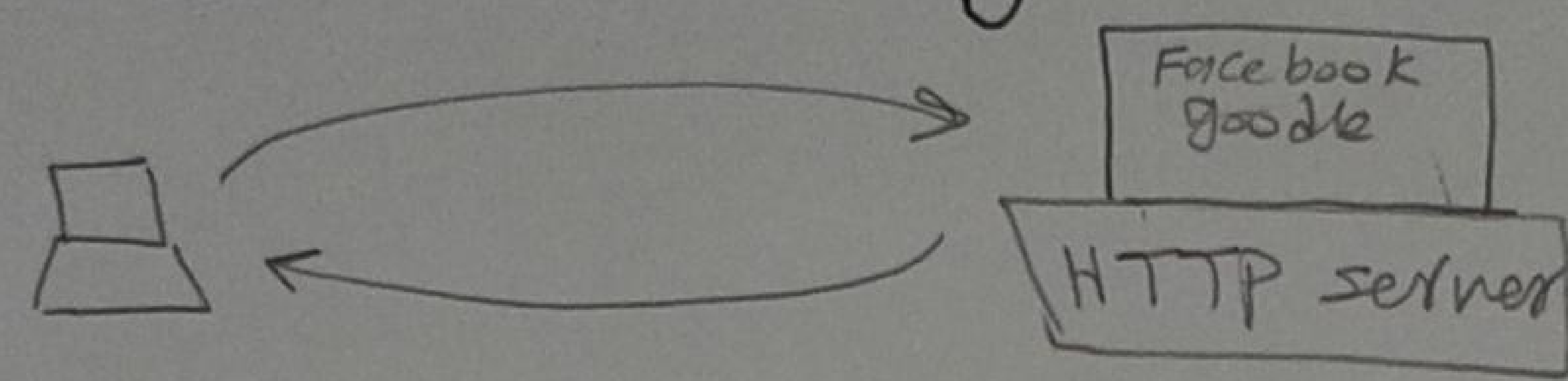
Examples of Network applications

> protocol is set of rules

EX1 HTTP (Hyper text transfere protocol)

Hyper text as [Text, pic, audio, vedio]

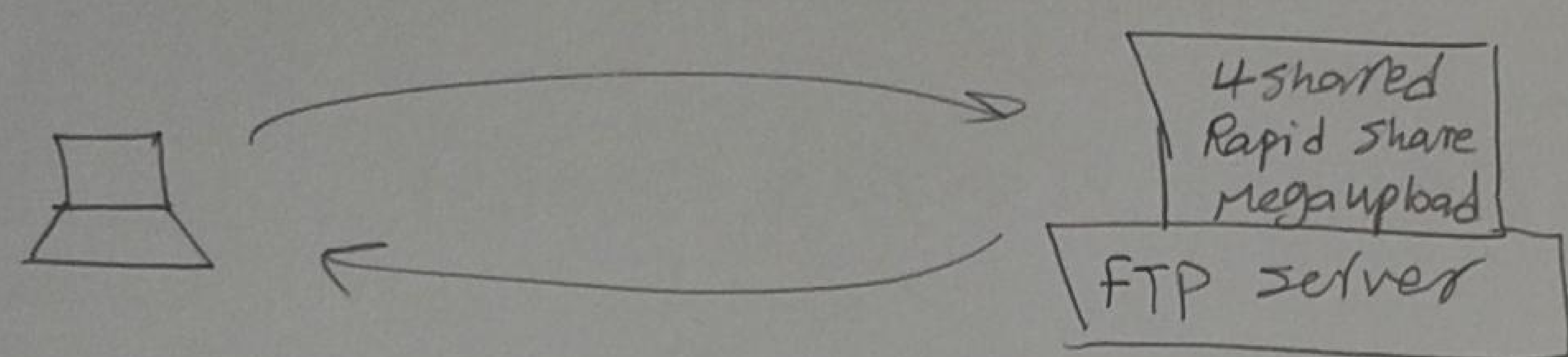
* it is used for browsing



EX 2 FTP (File transfere protocol)

File → Huge files

* it is used for upload and download data

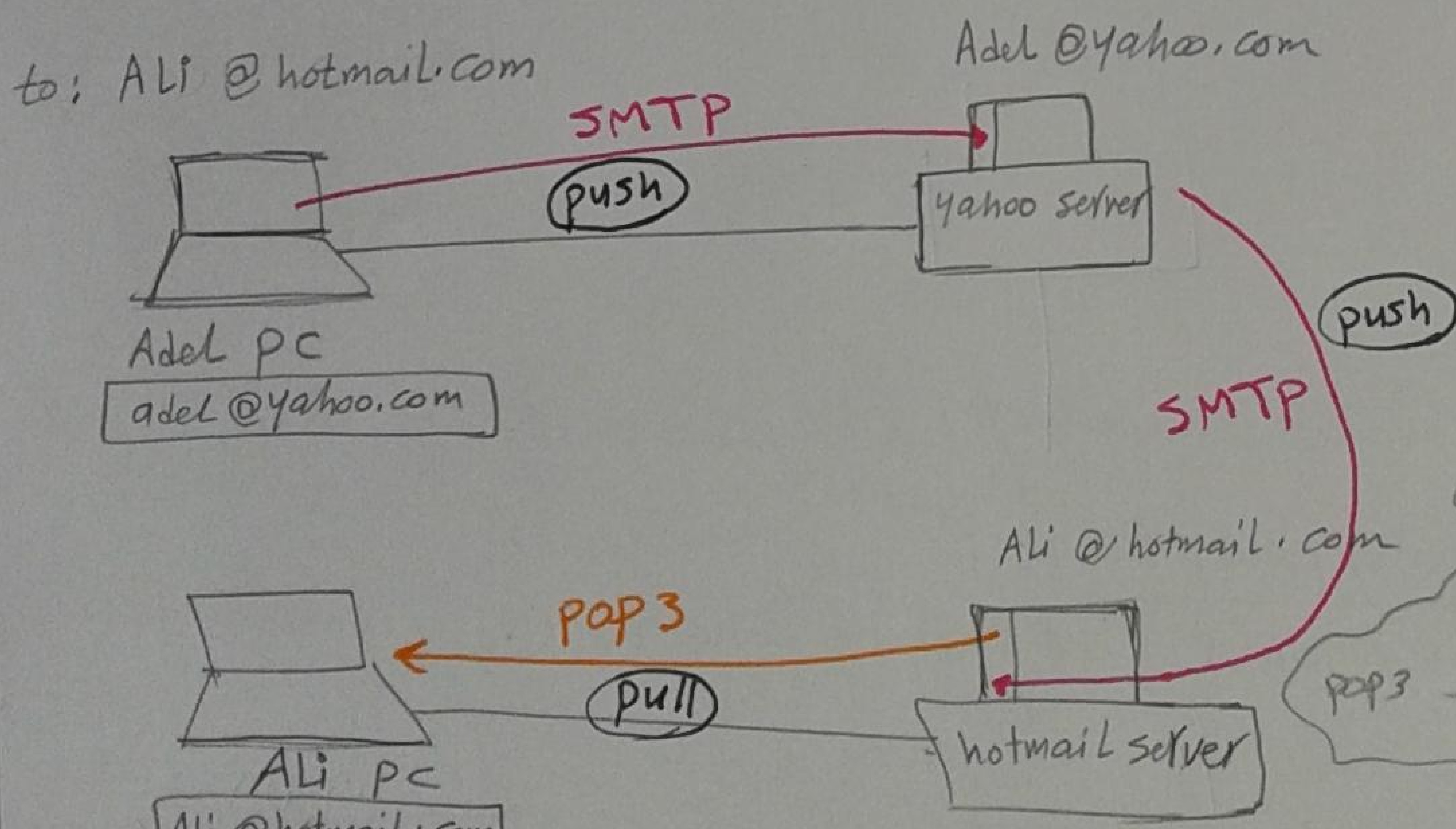


EX 3 Telnet

* It is used for remote login

EX 4
- SMTP (simple mail transfere protocol)
- pop 3 (post office protocol version 3)

} → used for using electronic mails



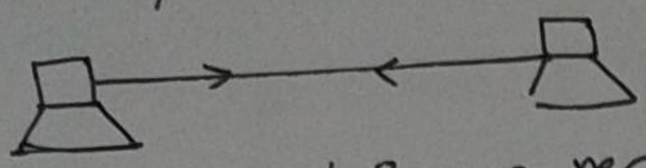
> انا عندى distination & source
> ومن حالتين
> ① لو ال dst. بيـ receive
> ال Mail ، يبقى بيعمل العمليه دى
> ال SMTP
> ② لو ال dst. بيسحب (retreive)
> ال Mail ، يبقى بيعمل العمليه دى ال pop3

SMTP is used for receiving Emails (passive)

pop3 is used for retrieving Emails (active)

Network Topologies :-

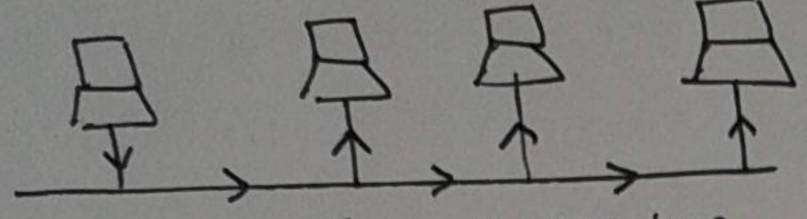
[1] point to point topology



one send & one receive

---

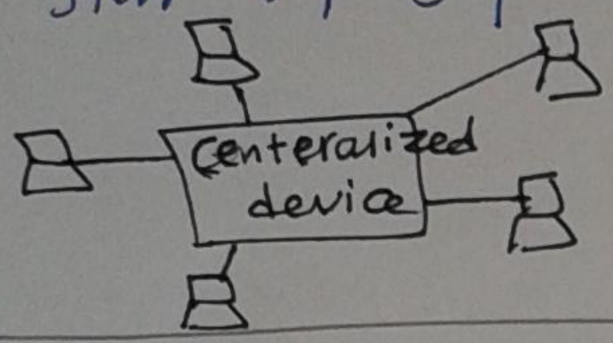
[2] Bus topology



one send , all receive

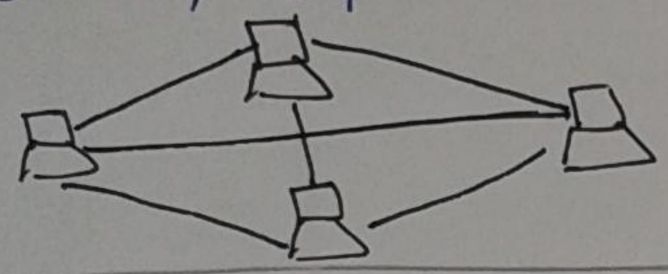
---

[3] Star topology



---

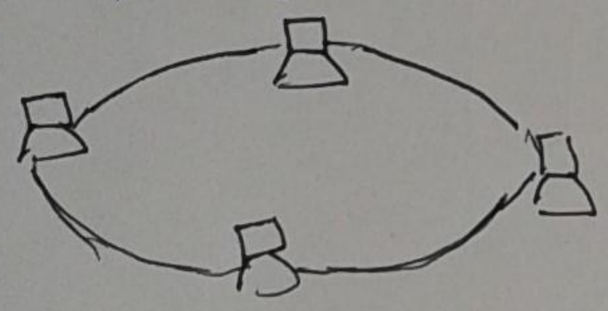
[4] Mesh topology



no of connections = $\frac{n(n-1)}{2}$

---

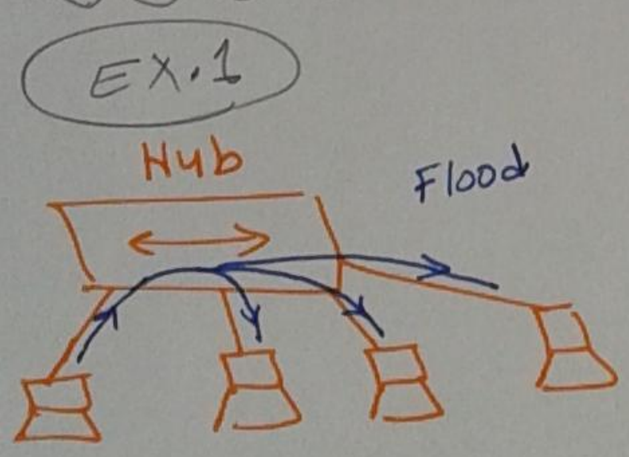
[5] Ring topology



---

physical topology v.s logical topology

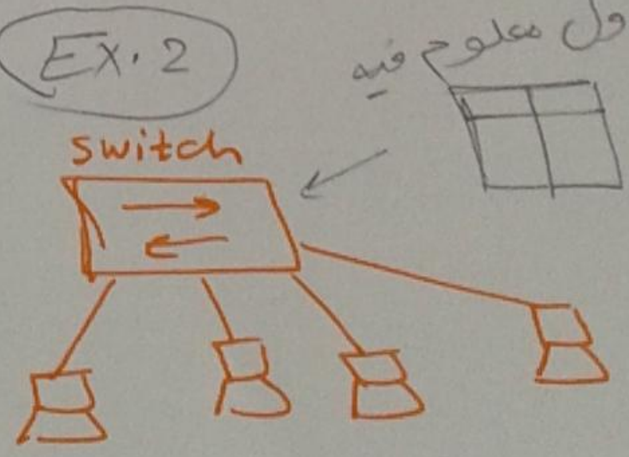
EX.1



physical : star

logical : Bus

EX.2



physical : star

logical : Mesh

Network types

LAN : local Area network

it is a group of Components connected one operator to gether in a small area

EX :

Ethernet → 10 Mbps

Fast Ethernet → 100 Mbps

GiGa Ethernet → 1 Gbps

10 GiGa ~ → 10 Gbps

MAN : Metropolitan area Network

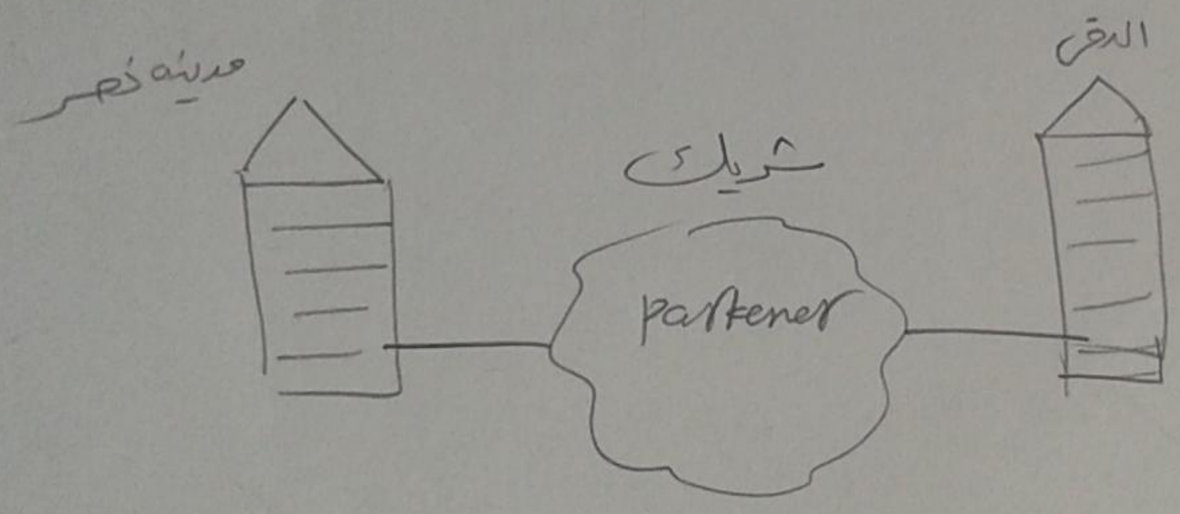
⇒ it is a group of LANs withen the same city

WAN : wide area network

⇒ it is Group of LANs between cities & contries & continents

⇒ Internet is the biggest WAN

EX : X.25
ATM
Frame relay



In case of partener, the LAN is converted to WAN

If there is no partenar, it is still LAN

Network is

group of component ---> connected together ----> to provide aservice

* end devices
- computer , IP phone , IP T.V , IP cam , play station

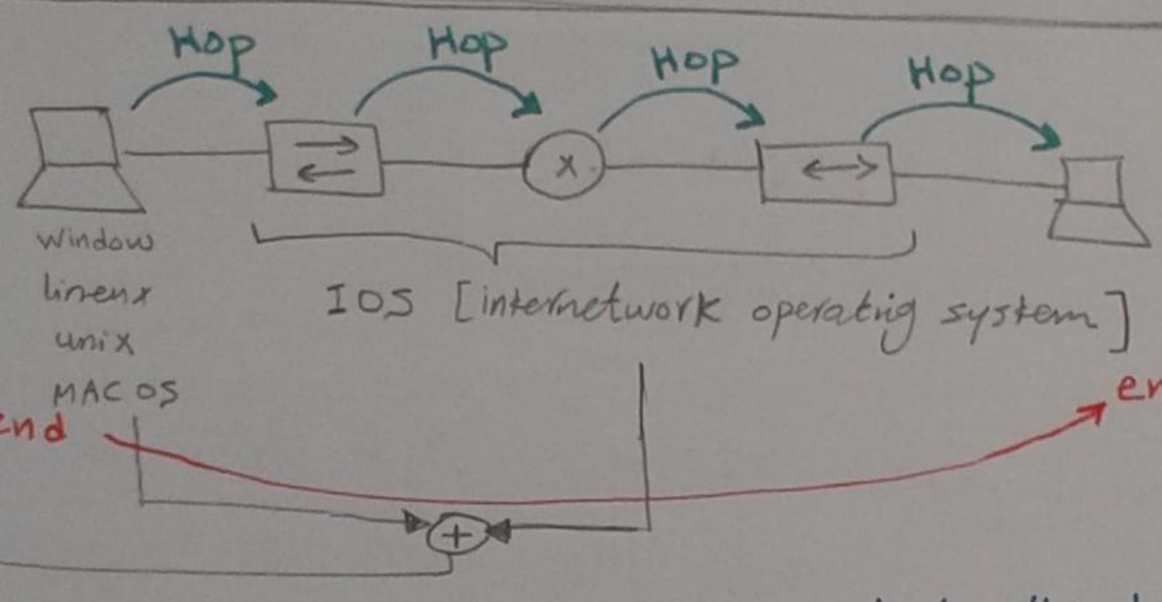
* Intermedite devices
- Hub , Router, switch

* connectivity

Topology
- point to point
- BUS
- star
- Mesh
- Ring

- data
- voice
- life
- vedio

LAN , MAN, WAN



Network Model / it is all concepts that will help the devices to know How to send data hop to hop and then end to end

Network model is some layer :-

* What is a layer? / it is a function that can be done either by S/W or H/W
* why layer ? / because functions are sequential

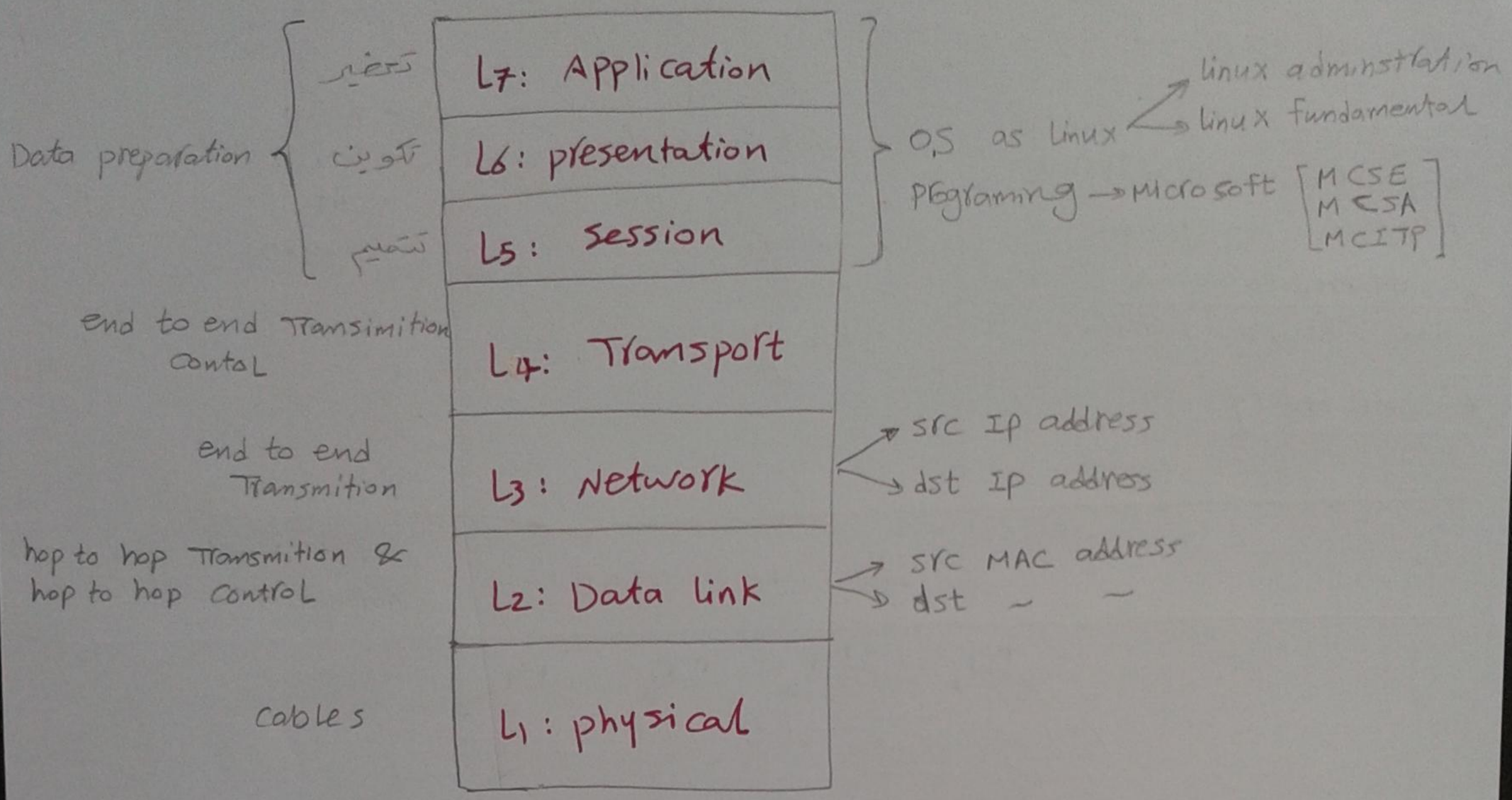
example of Network Models :-

① OSI Model [open system interconnection] developed by ISO and it is used as reference Model
open standard
open sourse

② Tcp/Ip [DOD Model] Department of Defence,
commertial Model ⇒ developed by DARPA وزارة الدفاع الامريكية

→ it is closed model
حتى مسموح لحد يطور فيه

OSI Model



L7 : Application layer : it is responsible for making the proper data preparation For the proper service

ex: service ⟶ application

Browsing ⟶ HTTP

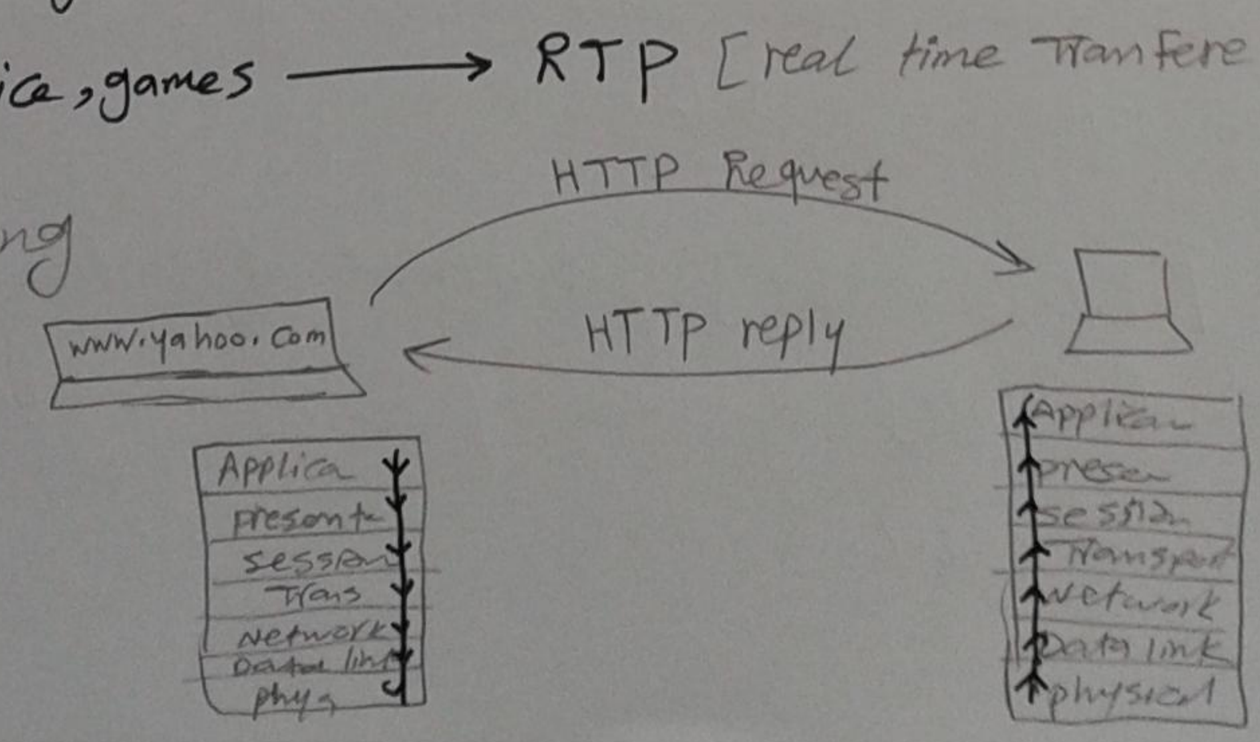
File upload & download ⟶ FTP

send / retrieve mail ⟶ SMTP / POP3

remote login ⟶ Telnet

Video, voice, games ⟶ RTP [real time Transfere protocol]

EX on Browsing



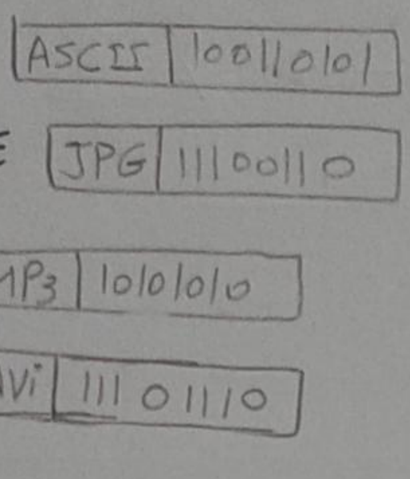
L6 : representation layer : it is responsible for finding common data representation between src & dst

Text → ascII

PIC → JPG , GIE

audio → Midi , MP3

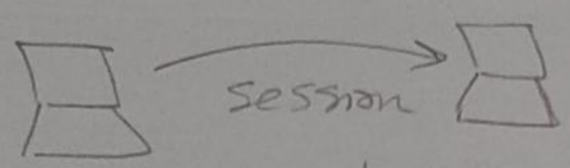
video → AVi , M pay



L5 : session layer : it is responsible for making sure that all information required for session opening become ready & in that case it will give orders for

العقل المدبر

1 - session establishment
2 - session Management
3 - session Termination



end to end communication.

Communiation يتأكد ان كل حاجه صح قبل ما يكمل

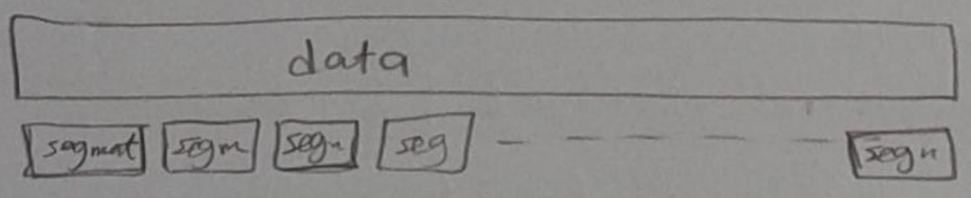
L4 : Transport Layer : it is responsible for the actual Mechanism of : ينفذ الاوامر

العمليات

1 - session establishment
2 - session Termination
3 - session managemant

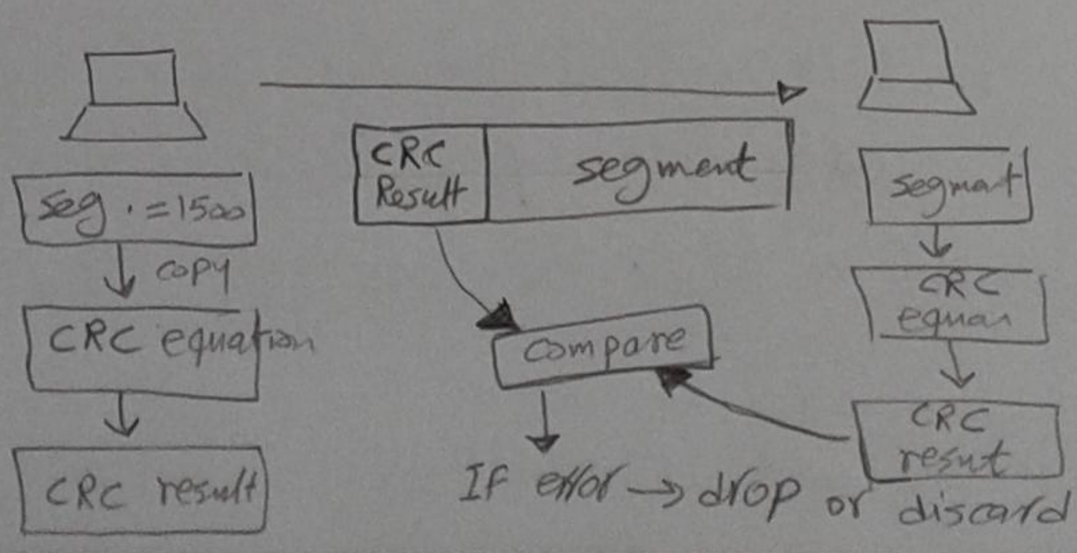
Transport layer function :-

[1] segmentation :- Deviding data into smaller segments



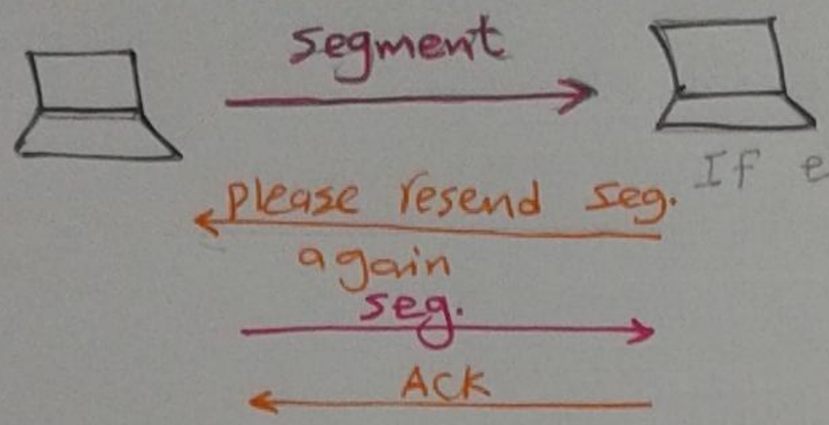
segment ≃ 1500 byte

[2] error Detection :- by CRC [cyclic redundancy check] = 4 byte



[3] segmentation sequancing :- giving serial no to each segment

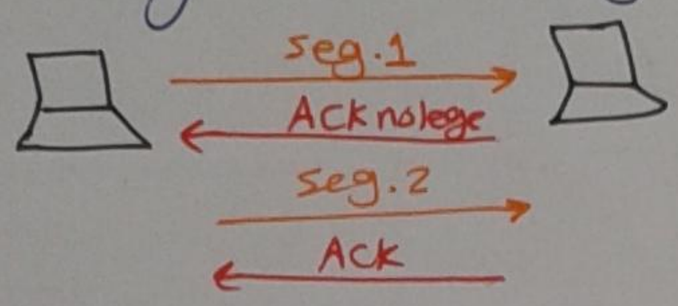
[4] error collection :-



---

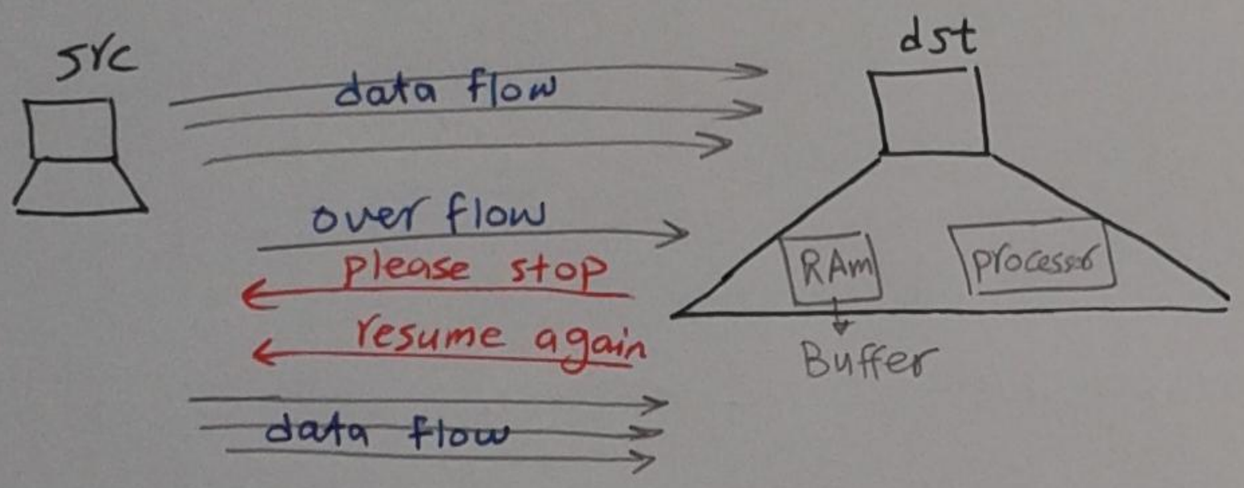
[5] Reliability :- Making sure that segments are correctly received

(Ack) بمعنى الرد بـ



---

[6] flow control



في حاله ان الـ RAm امتلت او الـ processor انشغل جداً ← الـ dst صيبعت رساله الى src ويقوله please stop ولما الشكله تتحل هيقوله resume again

---

types of s/w that is founed in Transport layer and excute all these steps above

[1] TCP : Transmition control protocol [يهتم بالدقة]
excute 100% of Transport layer functions [the 6 above]
used in HTTP, FTP, SMTP, POP3

[2] UDP : user datagrame protocol [يهتم بالانجاز]
excute 25% of Transport layer functions
used in RTP

L3 : Network layer : it is responsible for end to end data delivery

ex. of protocols Founded in L3 : IPv4, IP V6, IPx, Apple TAlk

it is responsible for → src IP address
dst IP address

IP address is an address used to identify end devices
[used as final end address]

L2: Data link layer / it is responsible for hop to hop data delivery and control

it is responsible for physical addressing and switching (finding the best path for next hop)

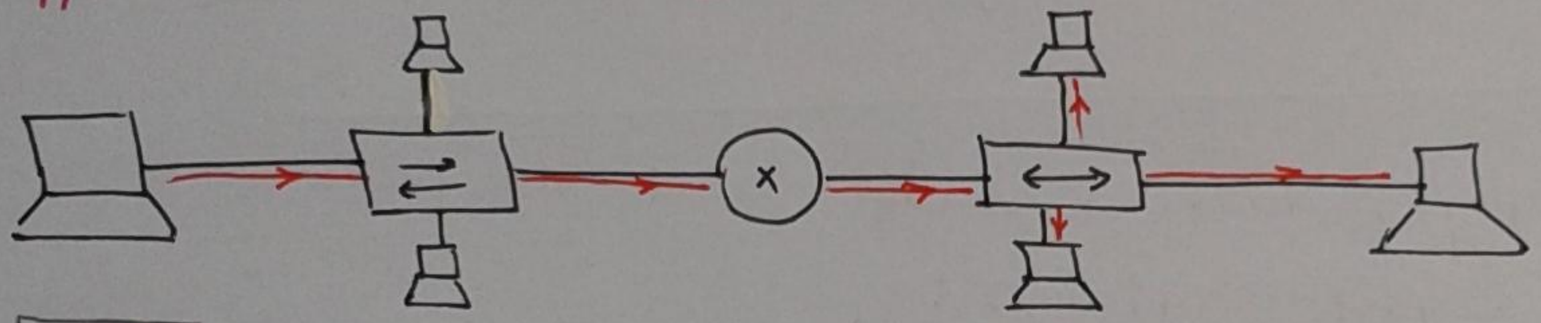
ex. of protocols Founded in Data link layer (L2)

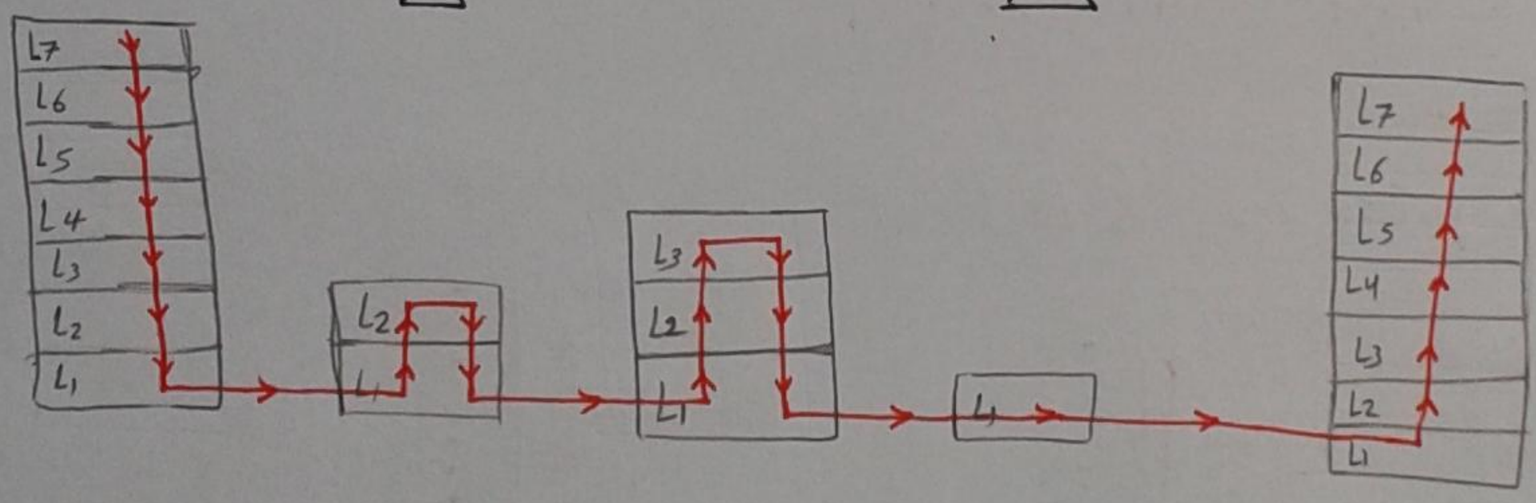
LAN
- Ethernet
- wi fi

WAN
- Frame relay
- X.25
- ATM
- DSL
- wimax

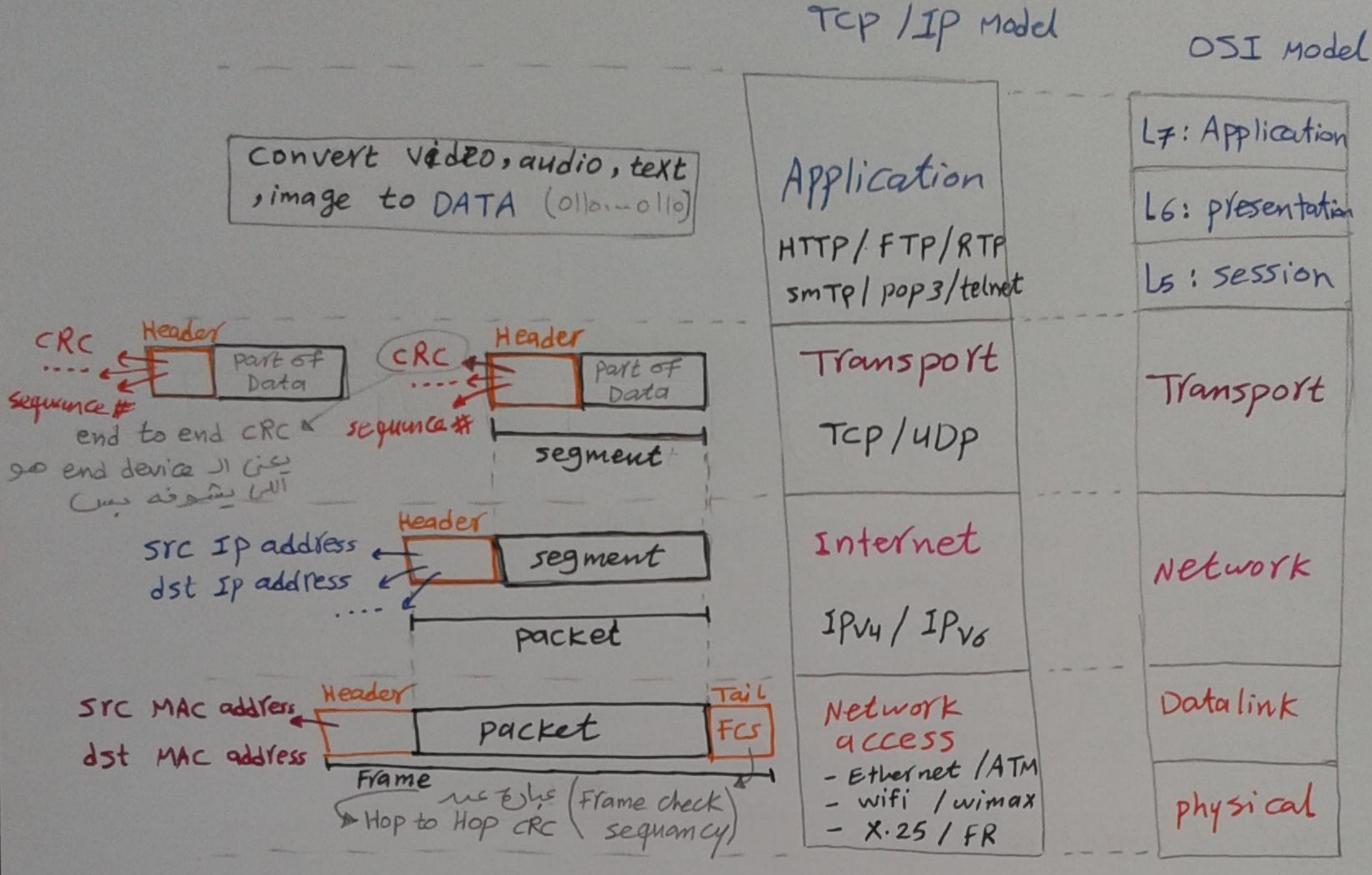
---

* Typical Network Model





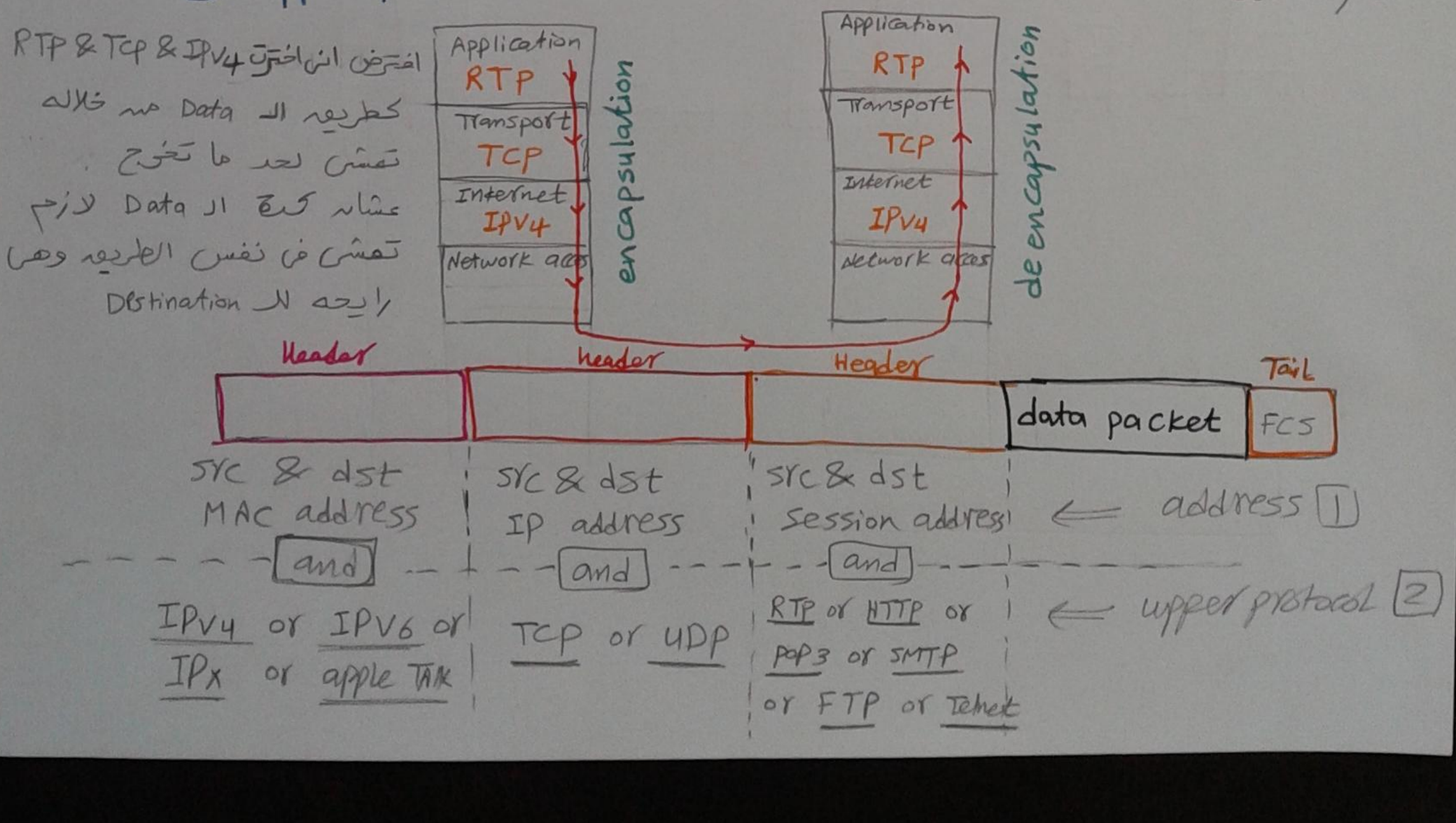
Note 1: layer 2 devices can by default understand layer 1
Note 2: when Data is drop, the device that wants it is the one who request for it



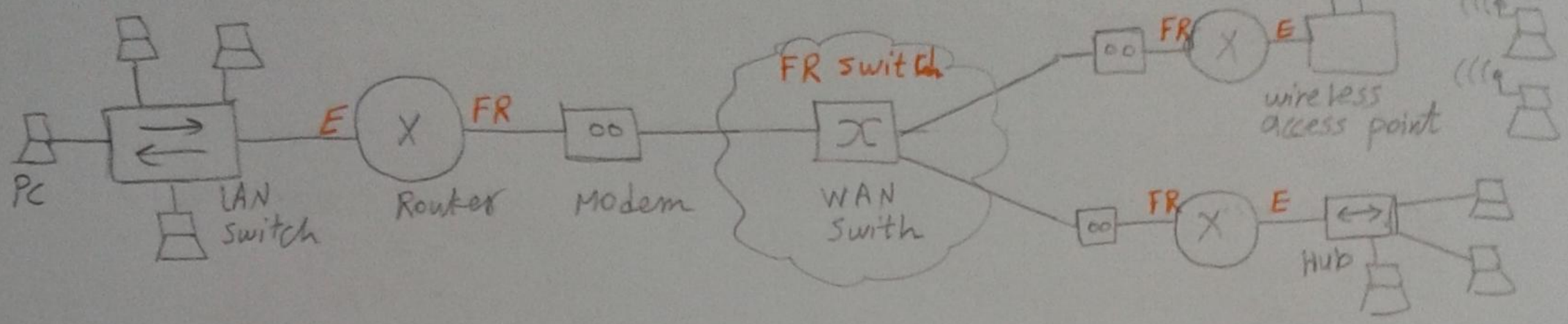
---

* Each layer adds a header to a data part , each header contains :-

1. address
2. upper protocol (pointer to upper protocol that is allready used before)



* Typical network components

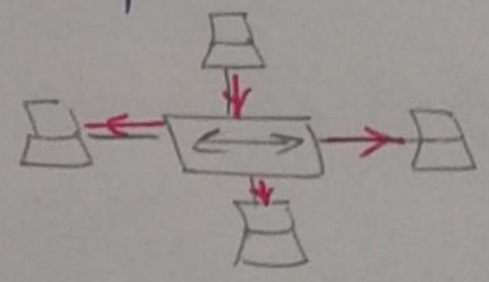


[1] Computer [end device]

* it is a soura of application
* it is L7 devica
* the proper physical topology is → Star topology

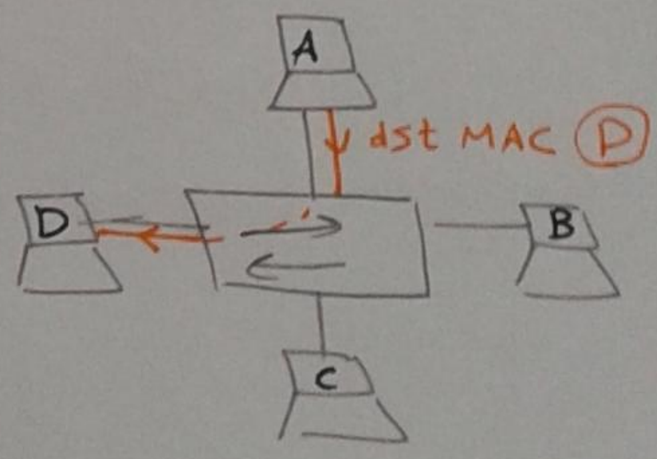
[2] Hub ⟷

* it is centeralized devica used to produce physical star topology
* it doesn't know neither Final address(Ip address)nore next hop(MAC address)
* it floods data / defining data out of all ports except the receiving port
* it is transparent devica (not a hop)



[3] switch ⇄

* it is a centeralized devica, used to provide a physical star topology
* it doesn't know how to reach Final end (IP address) but it knows how to reach next hop (MAC address)
* it is layer 2
* it is transperent devica (not a hop)



هو ملهوش MAC عشان كده كده ال Data لازم تمر عليه ولكنه عنده جداول يقدر منه خلالها يحدد ال Data رايحه فين (next hop) من خلال ال MAC اللى موجود فى ال packet

ملحوظه/ فى switch اسمه (Multi layer switch) ده يقدر يفهم لحد layer 7 وده حاجه advanced هنعرفها فى الكورس

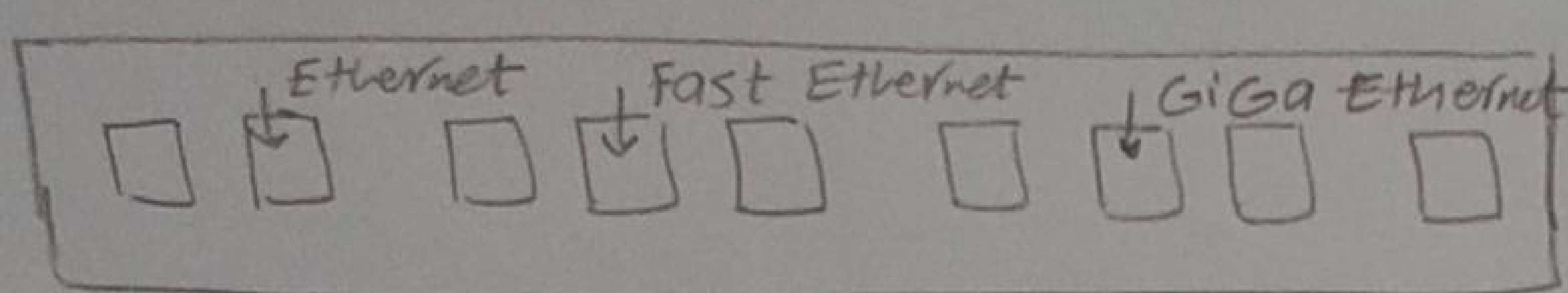
* all its ports of switch should use only single communi. Technology

يعني ان كل ال ports في ال switch الواحد مصنوعه من نفس التكنولوجيا

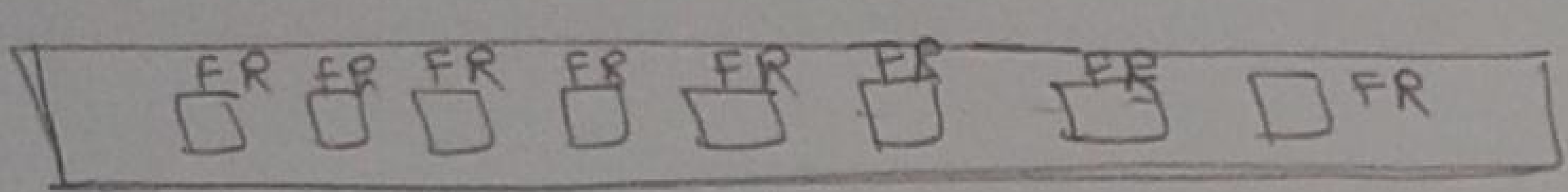
Communication Technology

LAN comm. Tech.	WAN comm. Tech.
- Ethernet	- X.25
- wifi	- FR
	- ATM
	- ISDN
	- DSL
	- wimax

(ex)

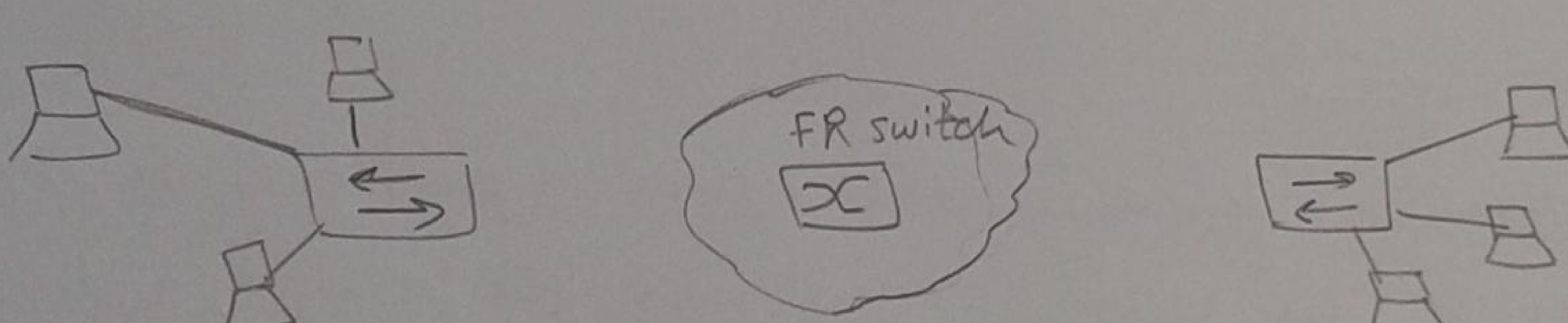


Ethernet switch



FR switch

المشكله هنا ان ال Ethernet له Max distance = 100M مينفعش استخدمه لمسافات طويله ، طيب لو رحت لل FR switch (WAN switch) ده هيحل مشكله المسافات لكن الكروت ال Network غاليه اوي و خليك فاكر ان كل ال ports في ال switch الواحد لها نفس Communication Technology



عشان المشكله دي ← اما استخدم كل 100m (switch Ethernet)
← او ادفع كتير اوي واستخدم (WAN switch) عشان ال fiber
وثمن الكارت اصلا غالي اوي

⇓

لازم اذهب الى ال **Router**

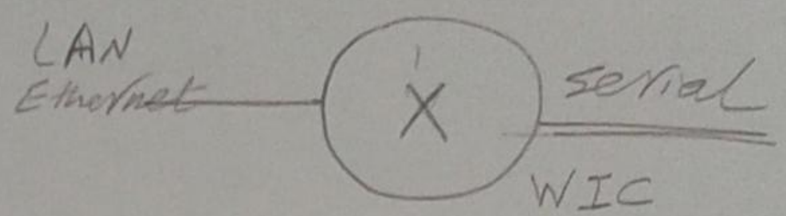
LAN switch	WAN switch
- high data rate	- low data rates
- cheap	- very Expensive
- lower range distance	- higher range distance

[4] wireless switch

* it is air switch
* it is layer 2

[5] Router

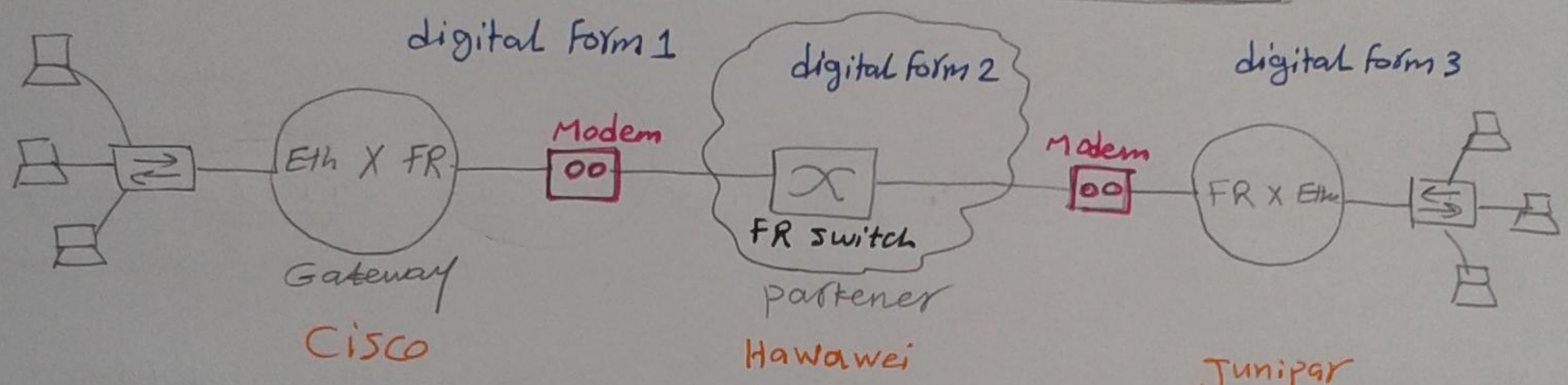
* it is a device that support multiple technologies by S/W
* it has interfaces LAN Technologies and WAN Technologies
* it can understand Ip address and MAC address
* the disadvantage of Router that it has more delay and very Expensive



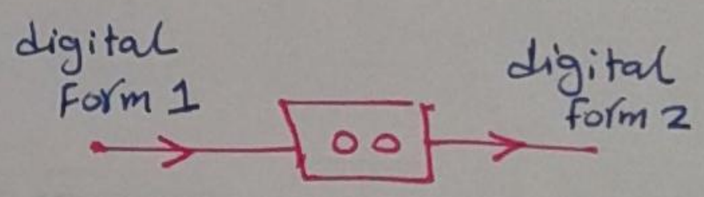
WIC : WAN Interface Card

- X.25
- FR
- ATM

!



[6] modem [modulator - demodulator]



It is used for :-

1- change digital forms ≡ line coding → to satisfy serveca provider

2- support clocking & syncronization

* it is layer 1 devica

note/ there isn't moden in LAN because in LAN, there is autoclocking in Ethernet that match clocking automatically

devices are classified in to

[1] DTE [Data terminal Equip.]

* it is adevice that can be either src or dst For data and information
* it should be at least layer 3

ex: PC & Router

[2] DCE [Date communication Equipment]

* it is adevica that can be either a centeralized devica or suppor clocking and syncromization
* it is at most layer 2

ex: Hub, switch, Modem, wireless access point

* physical layer [هيكون الكلام كله عن ال LAN]

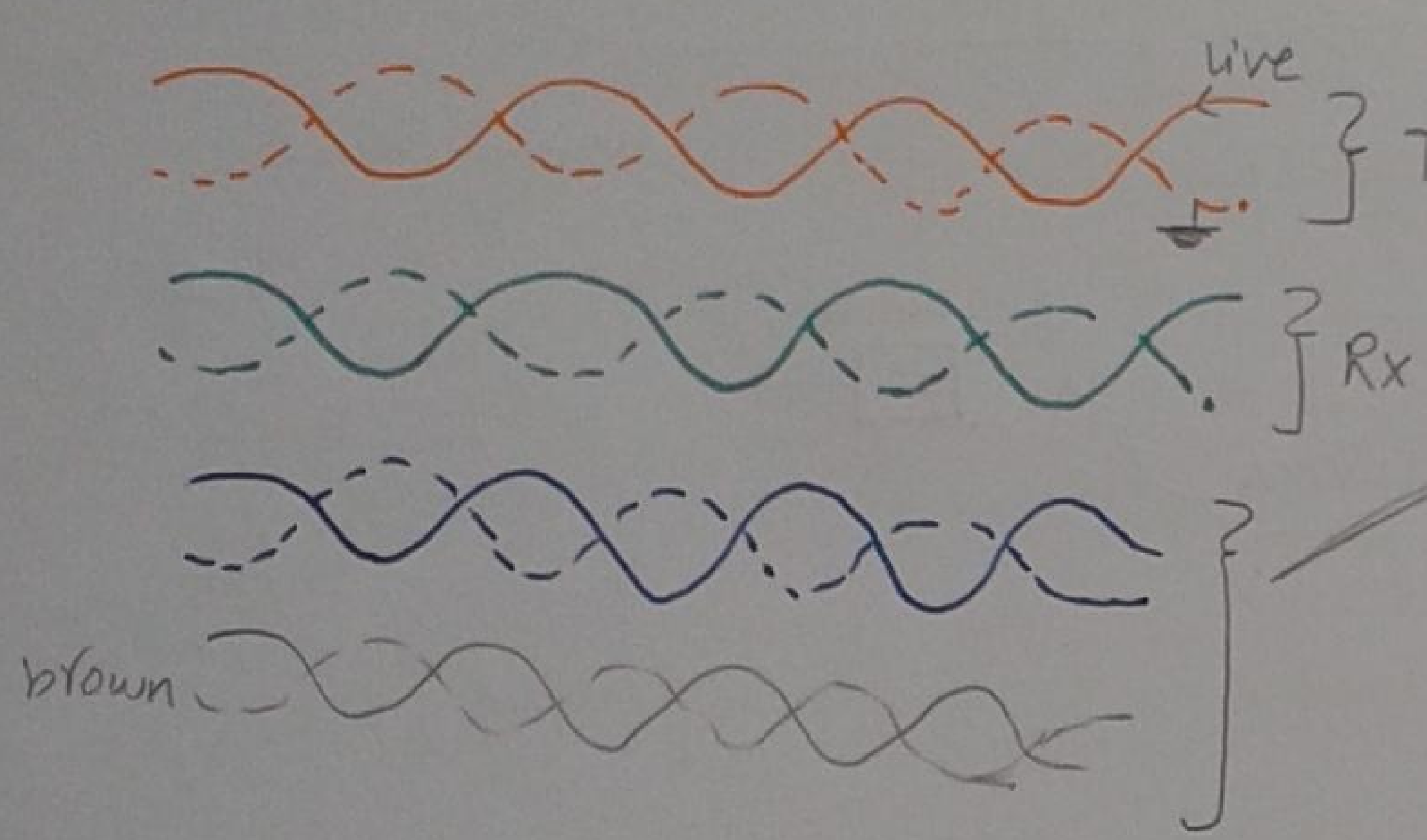
PDU [protocol Data unit] = Bits

LAN physical layer

- I — LAN Cables
- II — LAN Standard
- III — LAN connectors
- IV — LAN Devices

I LAN Cables

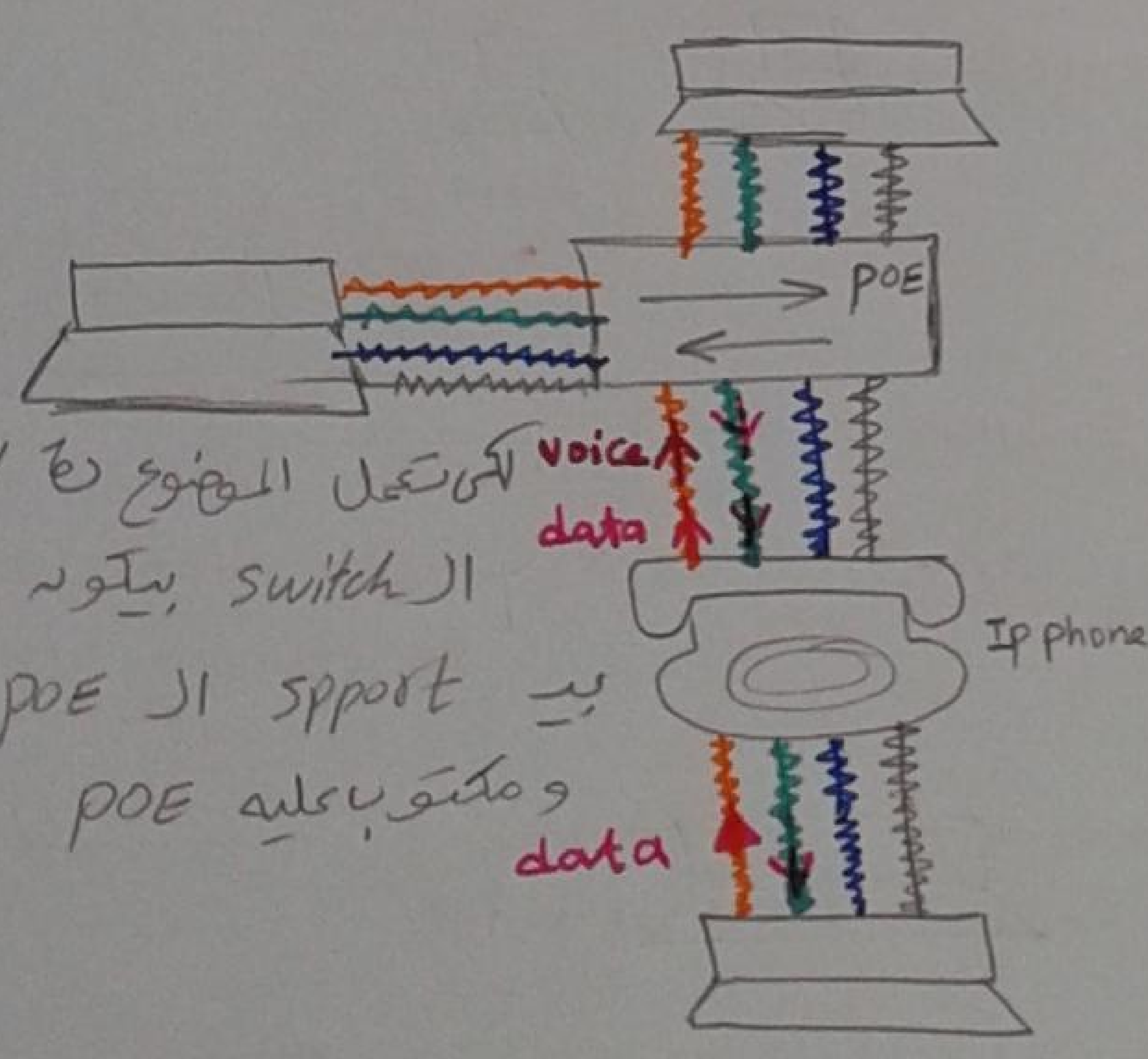
a UTP : unshilded twisted pair [8 wires e.g 4 pairs]



* بنستخدم ال blue & brown في حاله ال Very High Data rate ال مثلا GiGa & 10 GiGa Ethernet and POE [power over Ethernet]

* ال Ip phone له IP و MAC
* ال Voice بياخد 64 Kbps
لو الكابل بيشيل 100Mbps
→ 64 kbps for voice
→ The rest for data

* ال Voice دياماً بيسبق ال data



لكي تعمل الموضوع ده لازم ال switch بيكون بيـ sppoort ال POE ومكتوب عليه POE

* لو انت بتبعت بـ data rate زي ال Giga 6 كده انا بستخدم ال 4 pairs وبالتالي انا هخلي

Vcc = 5, GRN = 0 ← 3 pair

Vcc = 53, GRN = 48 ← 1 pair

وكده ال power متوصل لل Ip phone

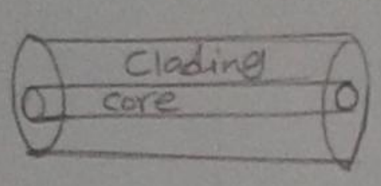
* the case of twisting
1- prevent electromagnitic interference and radio interference
2- prevent (cross talk) ← مشكلة داخلية
(e.g) cancle the existance of capacitance by inductance

[b] STP : sheilded Twisted pair

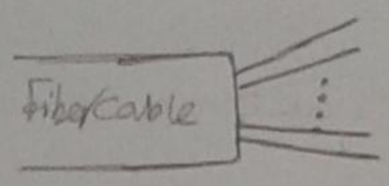
it is used to protect the signal from External low voltage difference
but If There is a high voltage difference, I have to use a Fiber

note/ both UTP & STP are used when maximum distance = 100 m

[c] Fiber



high light = 1
low light = 0



advantage of fiber ① Immunite against electric noise
② very high speed
③ support long distance
but it is very expinsive

Fiber

MMF (Multimode Fiber)
Core diameter = 62.5 Mm, 50 Mm
Cladding diameter = 125 Mm
400 m ⟶ 4 km

SMF (single mode fiber)
core diameter = 9 Mm, 8 Mm
Cladding diameter = 125 Mm
10 km ⟶ 100 km

* each device wants one pair of fiber wires, one for Tx & one for Rx

note / In LAN Network we don't use fiber because it is very expinsive
but we can use Ethernet that support speeds up to 10 GHz

[II] LAN Standards

IEEE 802.3 ⟶ standard for Ethernet
1980 February

Ethernet standard types :-

- 10 Base T
- 100 Base T
- 1000 Base T

← Twisted pair whose maximum distance = 100 m

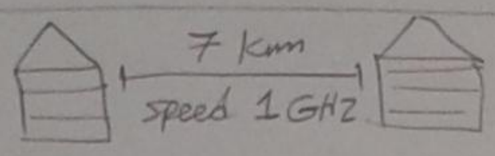
- 10 Base F
- 100 Base F
- 1000 Base SX — short distance → less 4 km [use MMF]
- 1000 Base LX — long distance → 10 km [use MMF]
- 1000 Base ZX — extra long distance → 100 km [use SMF]

← Fiber

speed in Mbps

Base band ≡ no need for Modulation

Interview question



what type of Ethernet that you should use ?? Choose 2 answers

sol :-

① 1000 Base LX → the best because it is cheaper and do the same work

② 1000 Base ZX

* twisted pair cable categories

- Cat 5 → 100 Mbps
- Cat 5e (enhanced) → 1 Gbps
- Cat 6 → up to 4 Gbps

] 100m

- Cat 6A (advanced) → 10 Gbps

] 25 m

- Cat 6E → 10 Gbps
- Cat 7 → up to 40 Gbps

] 100 m

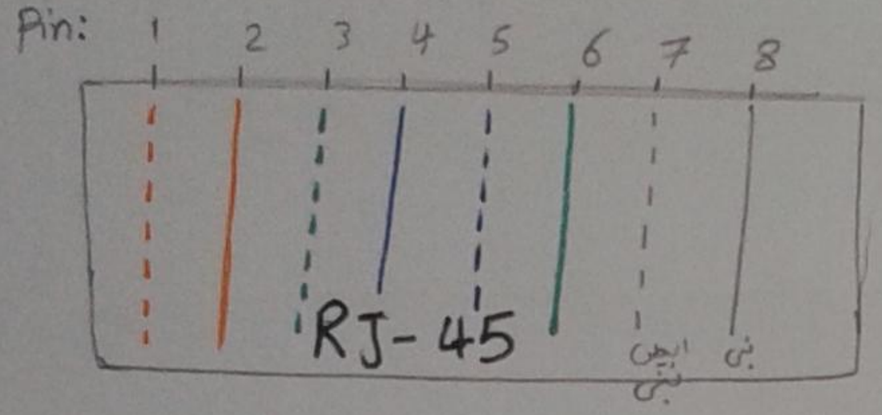
III LAN connectors

Fiber connectors

* ST : straight Tip
* SC : square connector

copper connectors

* DB : D-shaped [ex: DB-21 , DB-60]
* RJ : Register jack [ex: RJ11 , RJ45]



ملحوظة / الـ Data بتحب الالوان الفاتحه وبتستخدمهم لـ Tx & Rx ⇐ الالوان الفاتحه هى Orange & Green

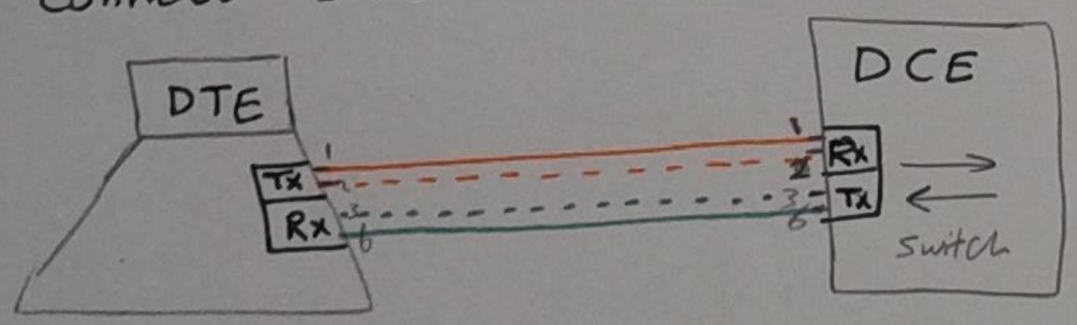
IP	This is a standard called T568A (Standard A)
Pin 1,2 → orange Pin 3,6 → Green	Pin 1,2 → Green Pin 3,6 → orange
This standard is called T568B (Standard B)	

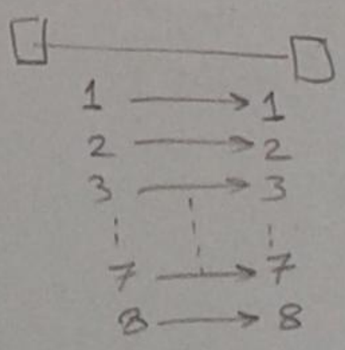
* Connection types :-

LAN DTE	LAN DCE
Tx : pin 1,2 Rx : pin 3,6	Tx : pin 3,6 Rx : pin 1,2
as PC & Router	as switch & Hub

1 Straigh Cables :-

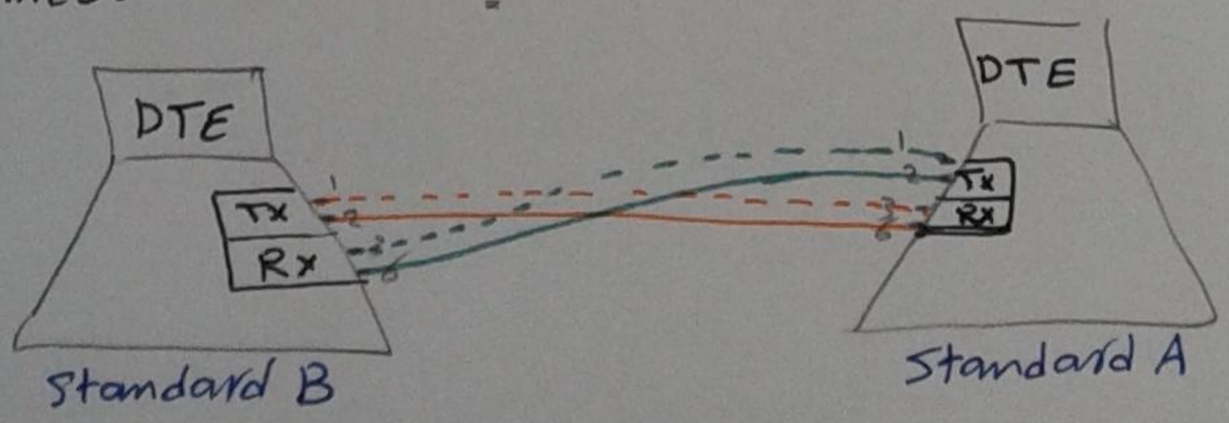
Connect DTE to DCE

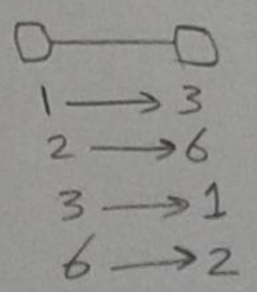




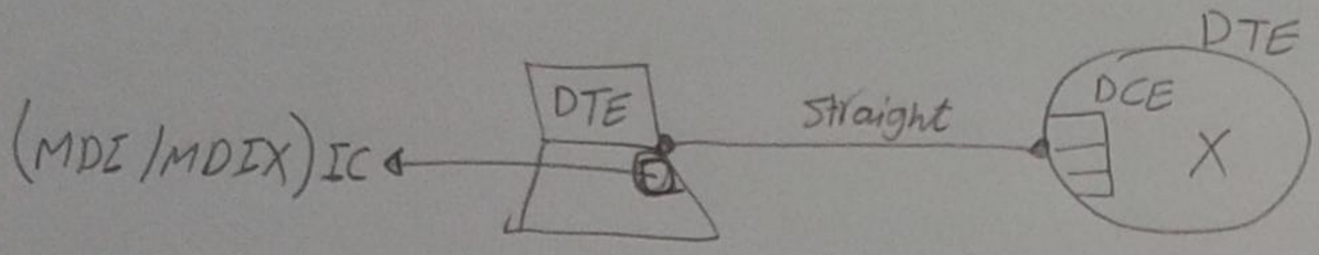
2 Cross Cable :-

Connect two DTEs or tow DCEs



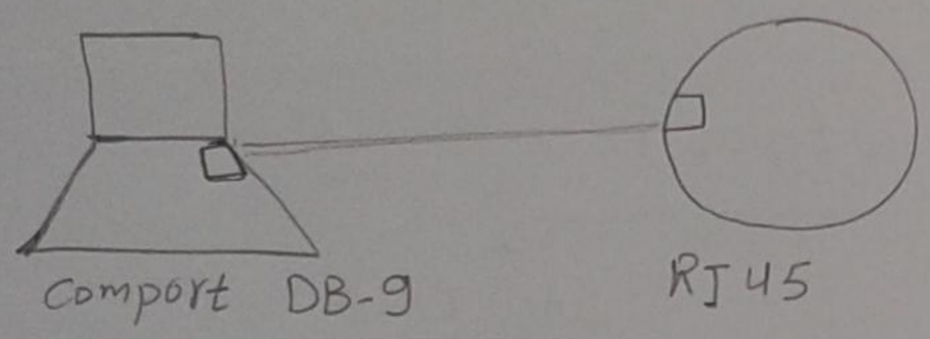


the Router in your home contain a built in switch, so that you can use a straight wire between your computer & Router and also the Router contains an IC that is called [MDI/MDIX] used for autosensing, then there is an option that you can Connect the cable whatever you want [straight or cross] and this IC will sense and correct the direction of Tx & Rx signals

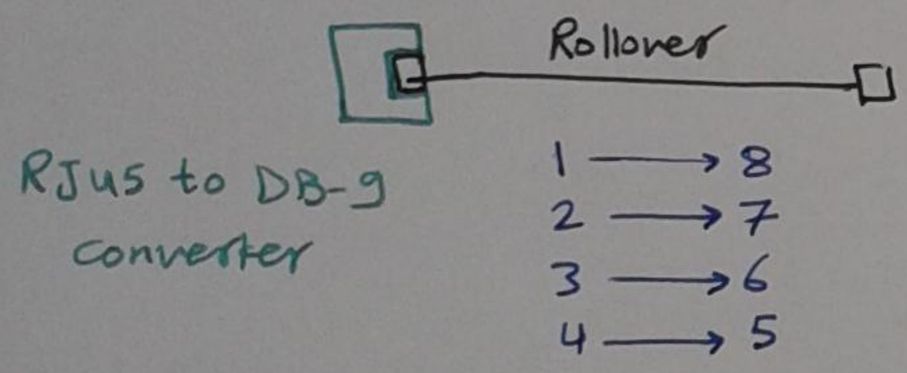


[3] Rollover cable [console cable]

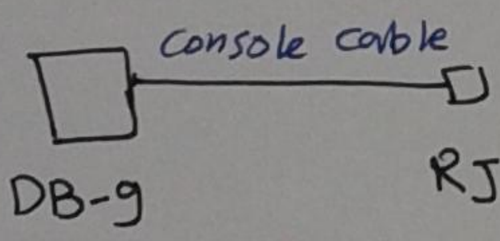
it is used for configuration only not for Data delivery



RJ-45 to DB-9 converter انت محتاج
كشان تحول من RJ-45 الى DB-9



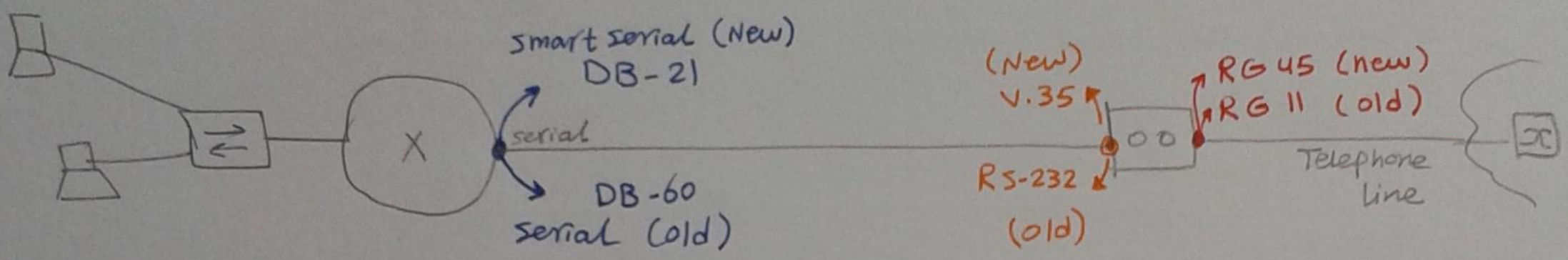
لو محتاجه تفصيل
Converter + Rollover

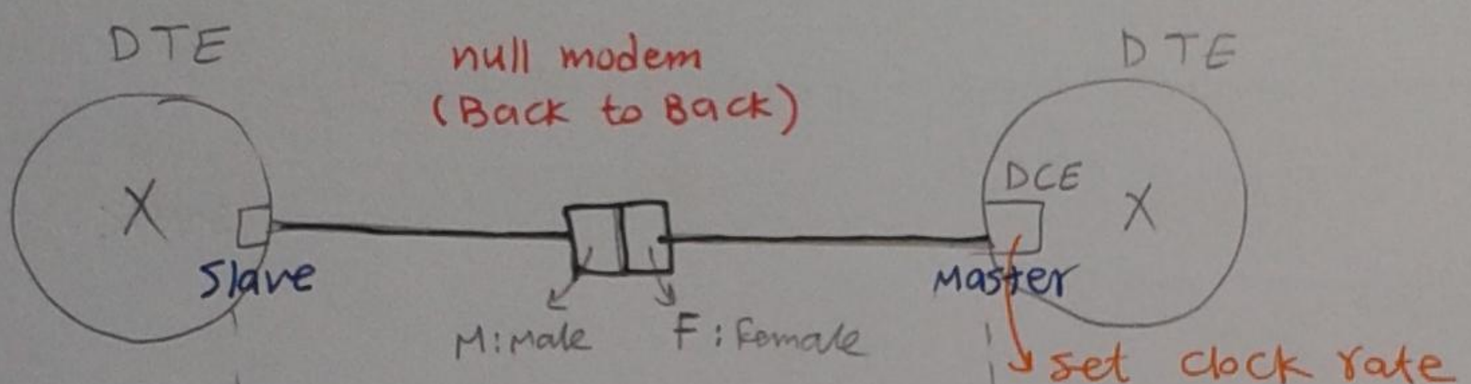


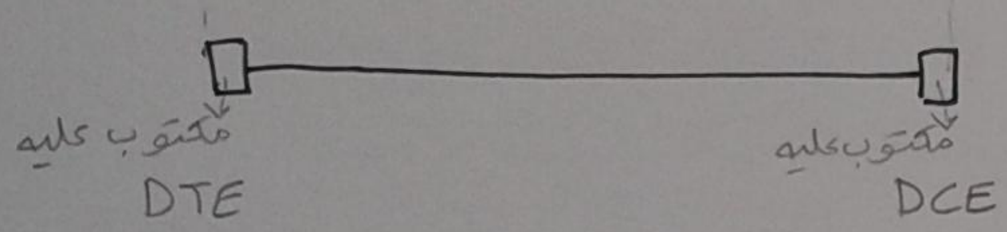
لو مشتريه جاهز هتشتري
console cable

* physical layer

PDU = Bits







الطرف اللي مكتوب عليه DCE

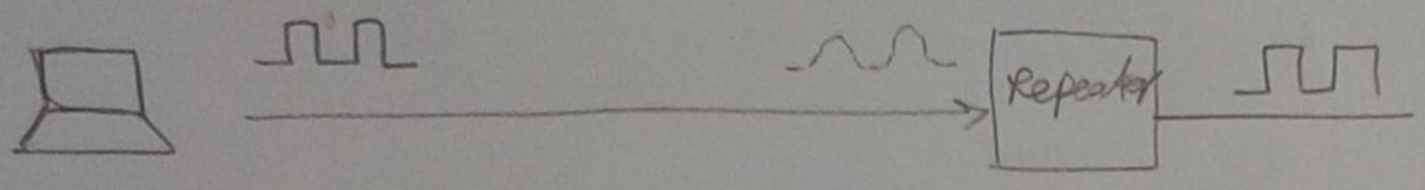
هروح على الروتر اللي متوصل بيه (DCE)

وهعمل عليه الـ set clock rate

* physical layer Devices

[1] Repeater

* it regenerates the signal * max no of ports = 4 ports
* I cannot use more than 4 repeaters because of the delay and collition



[2] Hub

* it is centerelized devica that support star topology ↔ advantage
* it is multiport repeater ←
* it floods data → disadvantage

[3] Modem

* Data link layer

delivery data & control problems from hop to hop

مسئول كلامنا صيكون عند الـ LAN وفي نهايه الكورس هنتكلم عند الـ WAN

[1] MAC address :-

[Network interface card]

it is an address that is burnt on NIC Rom , it is 48 bit address represented in hexa decimal , used to send & receive data hop by hop

1 bit hexadecimal = 4 bits

12 ~ ~ = 48 bits

* العيئه اللى بتنظم وتعطى ارقام الـ MAC هى IEEE

[organization unique Identifier] OUI ≡ vendor part (24 bit) | host part (24 bit)

XXXXXX XXXXXX

12 bit hexadecimal

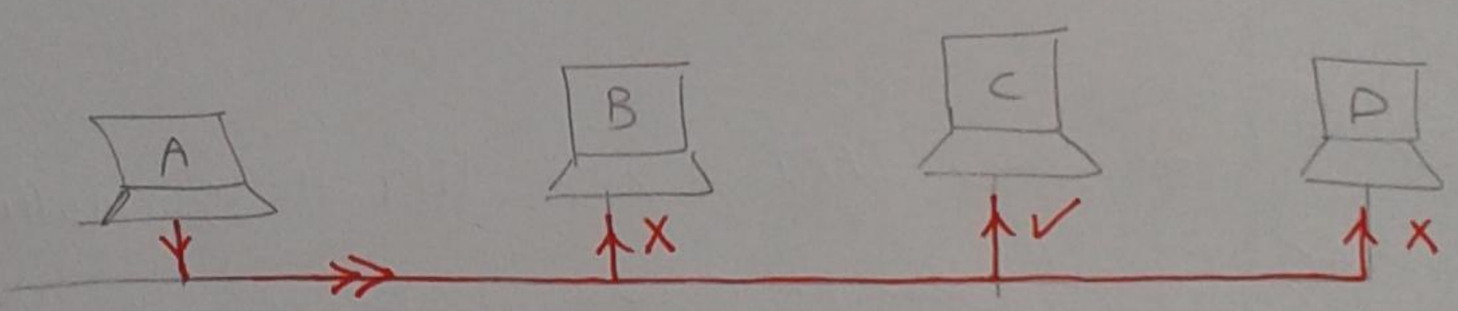
* Cisco has 32 vendor part

Types of destination MAC

[A] unicast MAC

A → C

one send & one process

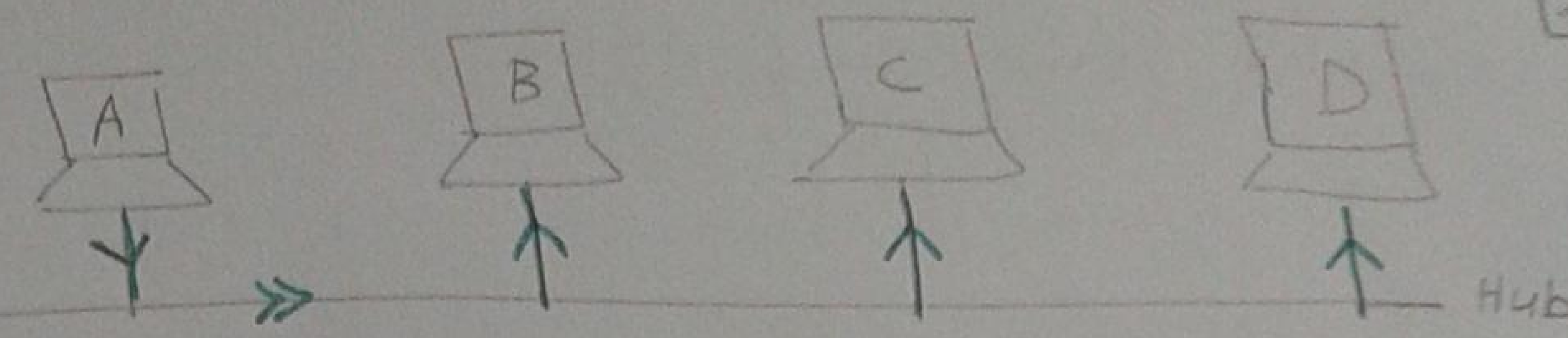


Example of unicast :-

- HTTP → لاني بـ Browse هبعت لجهاز واحد
- FTP → ~ بـ DL او UP هبعت لجهاز واحد
- SMTP → نفس الحكايه
- DNS

b Broadcast MAC

destination
FFFF FFFF FFFF



one send & all receive and process

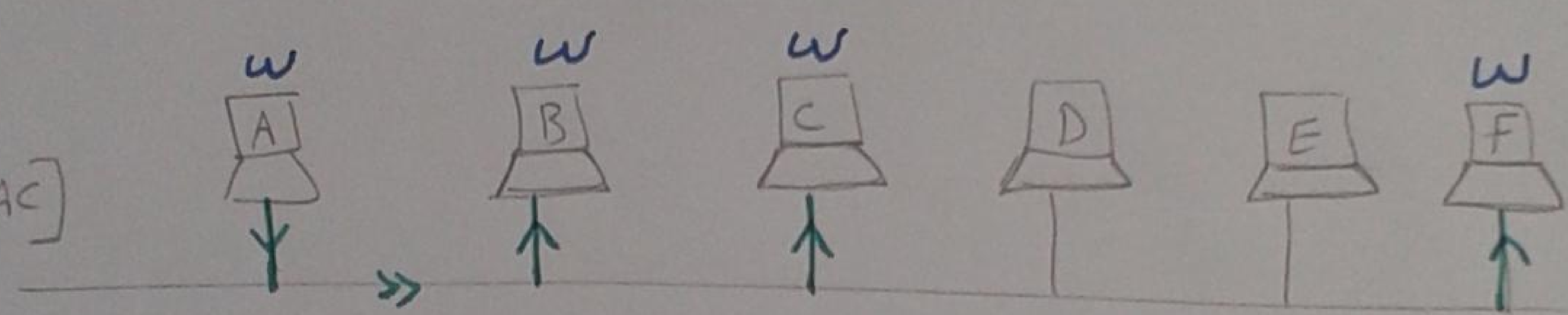
* كل NIC فيه MAC خاص بيه و MAC عام كله FF...FF عشان ال Broadcast

note
* Flood ⇒ all devices receive the data but some only can process
* Broadcast ⇒ all devices receive the data and they must process it

بمعنى ان ال Broadcast بيجبر كل الاجهزة انها ت process الداتا

c Multicast MAC [application games]

destination ω
[ω is the multicast MAC]



one send & some receive and process

* اى Multicast application زى ال Fifa بتروح ال IEEE وتطلب منها اكتر من MAC address عشان كل مجموعه بتلعب Game مع بعض ياخدوا MAC معين والـ MAC ده بيكون vertual MAC يعنى مبيكنش مطبوع فى NIC بتاع جهازك لكن ال application بتسطب ال Mulicast MAC فى ال RAM اثناء ال Game

then every NIC card has more than one MAC address

1- unicast MAC
2- Broadcast MAC
3- Multicast MAC If you play a Game and If you play 1000 application then ~~you~~ have 1000 unicast MAC address for them

2 MAC Method

CSMA/CD : Carrier sense Multiple access with Collision Detection

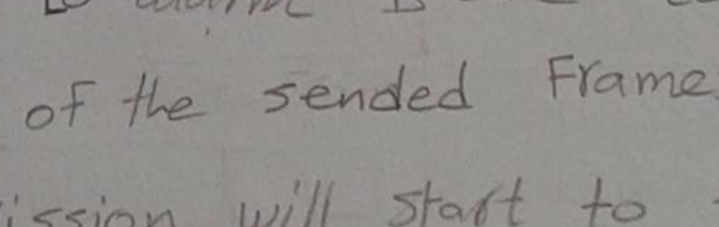
* CSMA is the brother of CDMA & TDMA & FDMA and it is the oldest of them
* CSMA is found on NIC
* we use it in case of using the Hub and wireless but we don't use it in case of switch

طريقة عمل الـ CSMA

If I need to transmitte , first I should sense the receiver

- If Rx is busy ⟶ stop Tx
- If Rx is free ⟶ start Tx

note / all devices on a hub should operate half duplex
[e.g either TX or RX at atime]

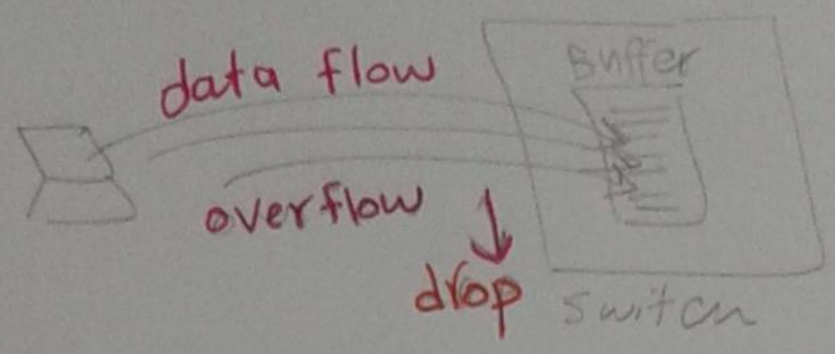


نكمل في مثالنا السابق

* IF A & D send in the same time , collission will take place then A & D will be the first to detect the collission because they found themselves can both send and receive
* then A & D will start a back off algorithem [will stop sending]
* A & D send jam signal [إشارة تشويش] to alarm B & C to the collission to cancel the operation of the sended Frames
* then each device that sensed the collission will start to transmitte in a random time to prevent a new collission again

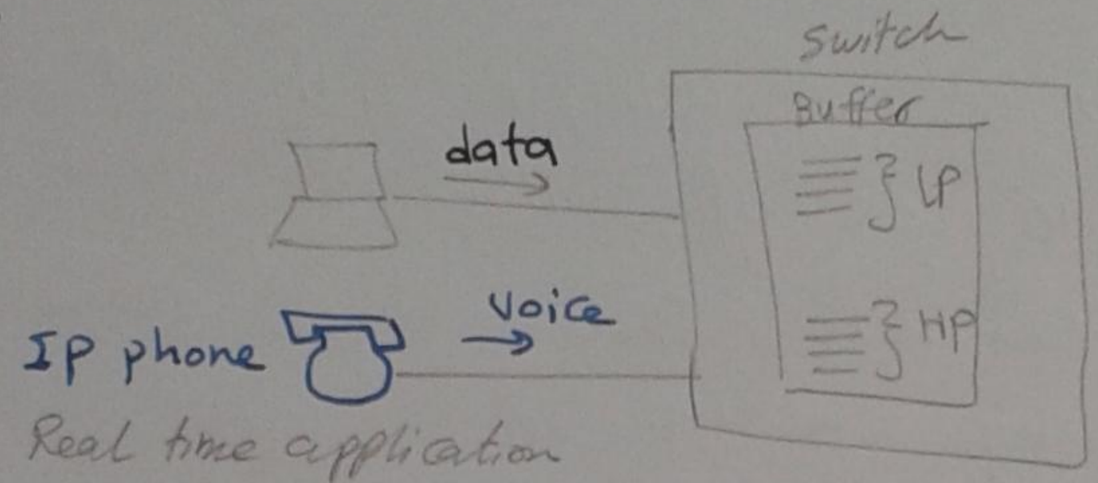
[3] MAC Flow Control

[a] Buffuring



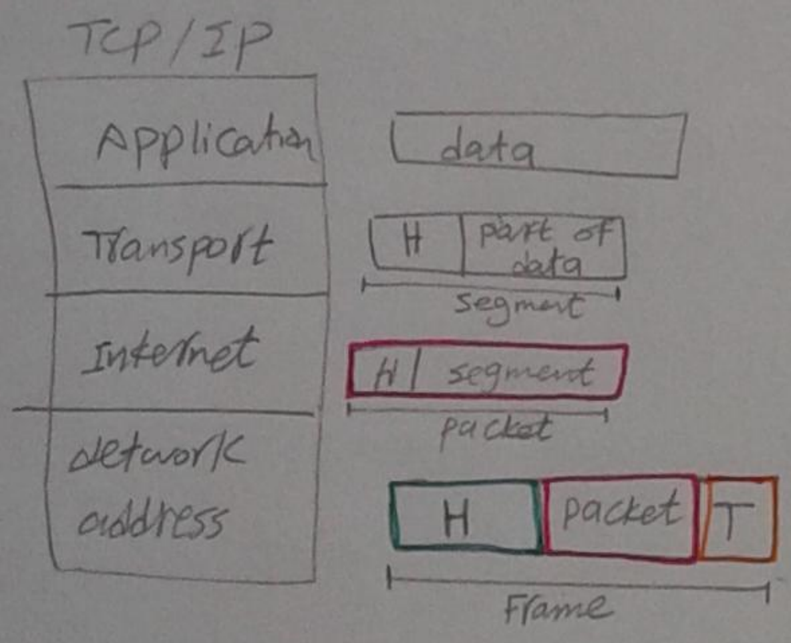
[b] Congestion avoidance تفادي الاختناقه

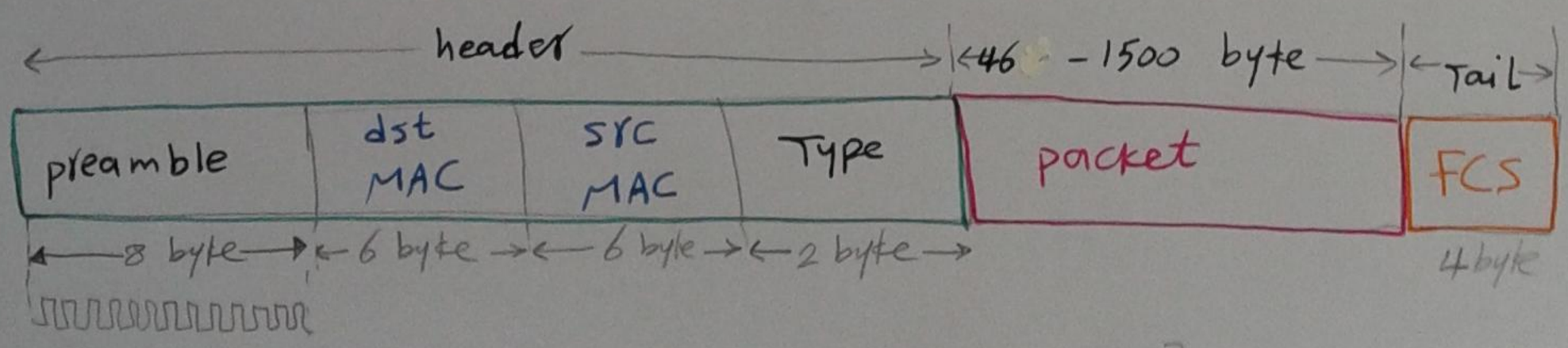
→ drop low periority



- it gives the Data low periority and the voice high periority
- If the memory is full, it deletes the low periority data to serve the high periority voice, because I can resend the data again but I can't resend the voice to be transparent to user

[4] MAC Frame





FCS : Frame check sequance [it is as CRC]

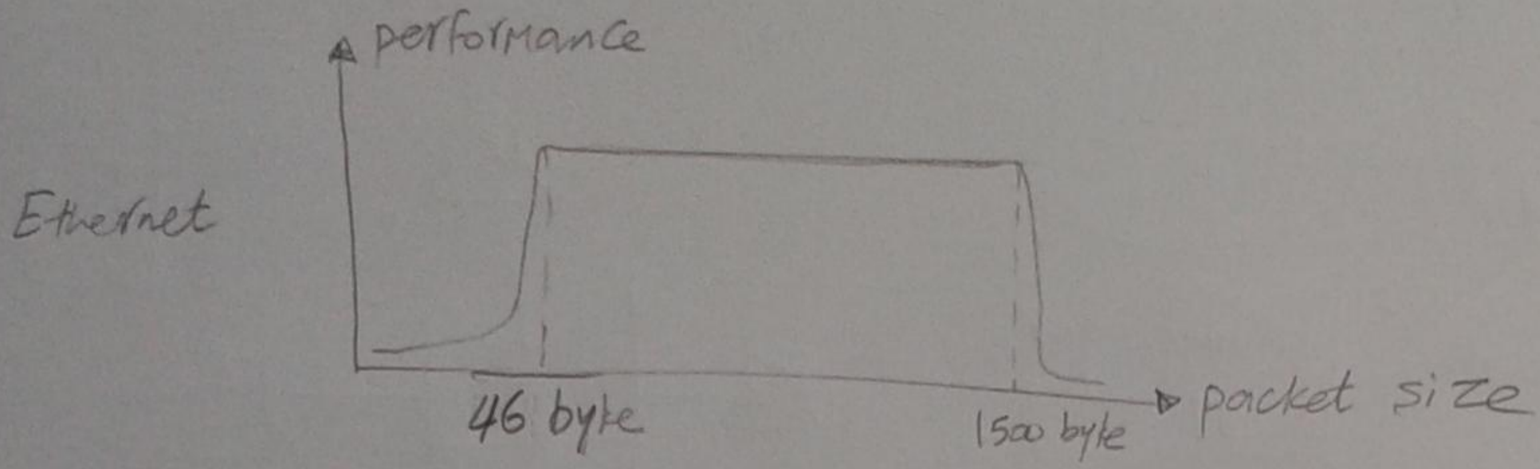
note 1

* the preamble is used to determine the autoclocking

If it is → 100 Mbps / 1 Gbps / 10 Gbps for Ethernet, and it is sent at the start of sending only

not 2

* performance V.S packet size For Ethernet



MTU : Maximum Transfere unit

not 3

type (type) : Contain the name of upper incapsulated protocol

ex: IPV4 or IPV6 or IPX

كمثال يقول الداتا جت منين

and also it contains the length of frame

Then the frame size → min: packet + H + T = 64 byte
→ max: paket + H + T = 1518 byte

5 layer 2 devices

Devices understand MAC

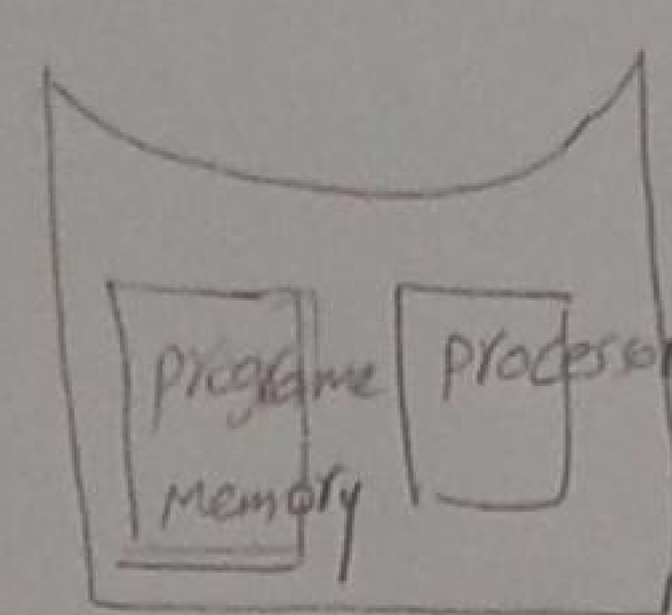
- address
- Frame
- method
- Flow Control

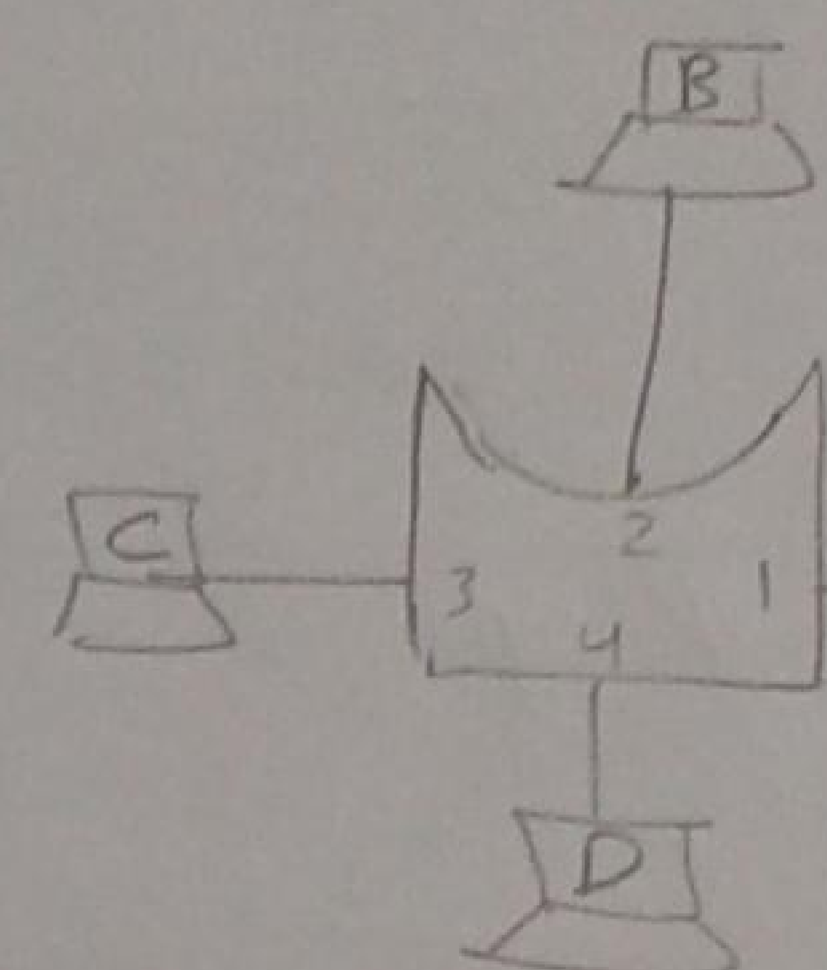
1 NIC: [Network interface card]

→ it has MAC

2 Bridge:

- it acts as intelegent repeater
- it builds a MAC table
- max no of ports = 16 port
  (this no is very limited
  → dis advantage of bridge)
- it operates by S/W



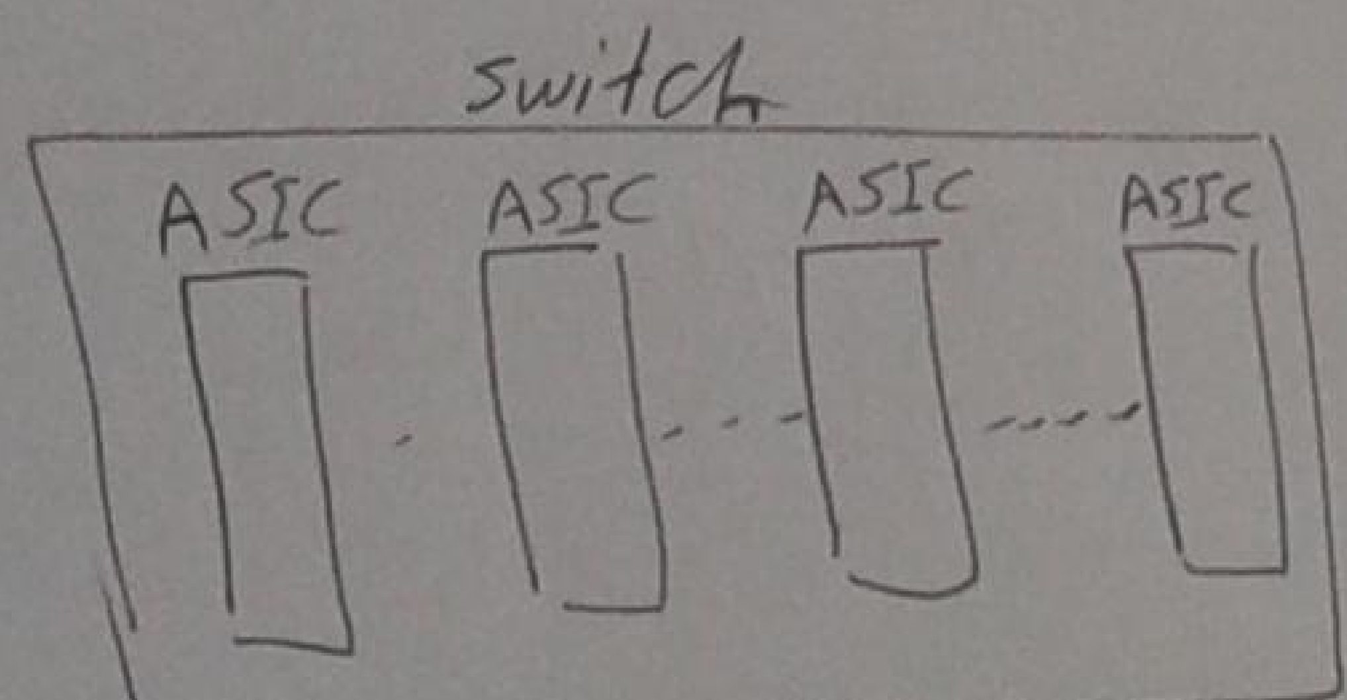


MAC	port
A	1
B	2
C	3
D	4

ودة معناه ان عشان تنفذ كل Frame ← لازم ال Frame دي تمر على S/W
ينفذها ودة بيخلي ال Bridge بطيء جدا وقلل كمان عدد ال ports
اللي فيه عشان ال Bridge مش يهنج

3 Switch

- it is multiport Bridge
- it operates using H/w ASICs [Application specific integrated circuits]



* Each ASIC has a specific job

Cisco Catacyst 6513
576 port
720 Gbps
↓
1.4 Tbps

Juniber EX-8216
786 port
6 Tbps
↓
12 Tbps

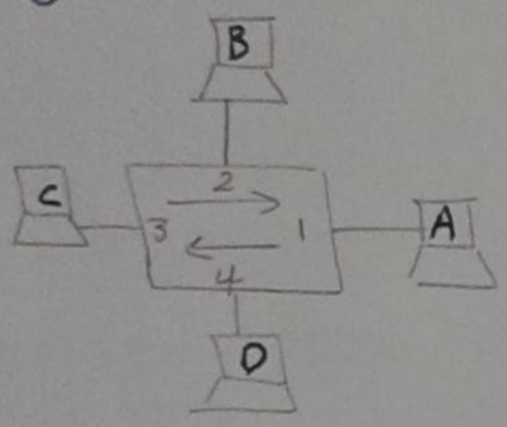
Cisco NexUD
8xx port
12 Tbps

→ Tera ≡ 1000 Giga

switch operation → learning through SRC MAC
→ Forwarding through DST MAC
→ Remove L2 loops
↓ layer2

1 learning

Forming MAC table by checking SRC MAC in any incoming Frame

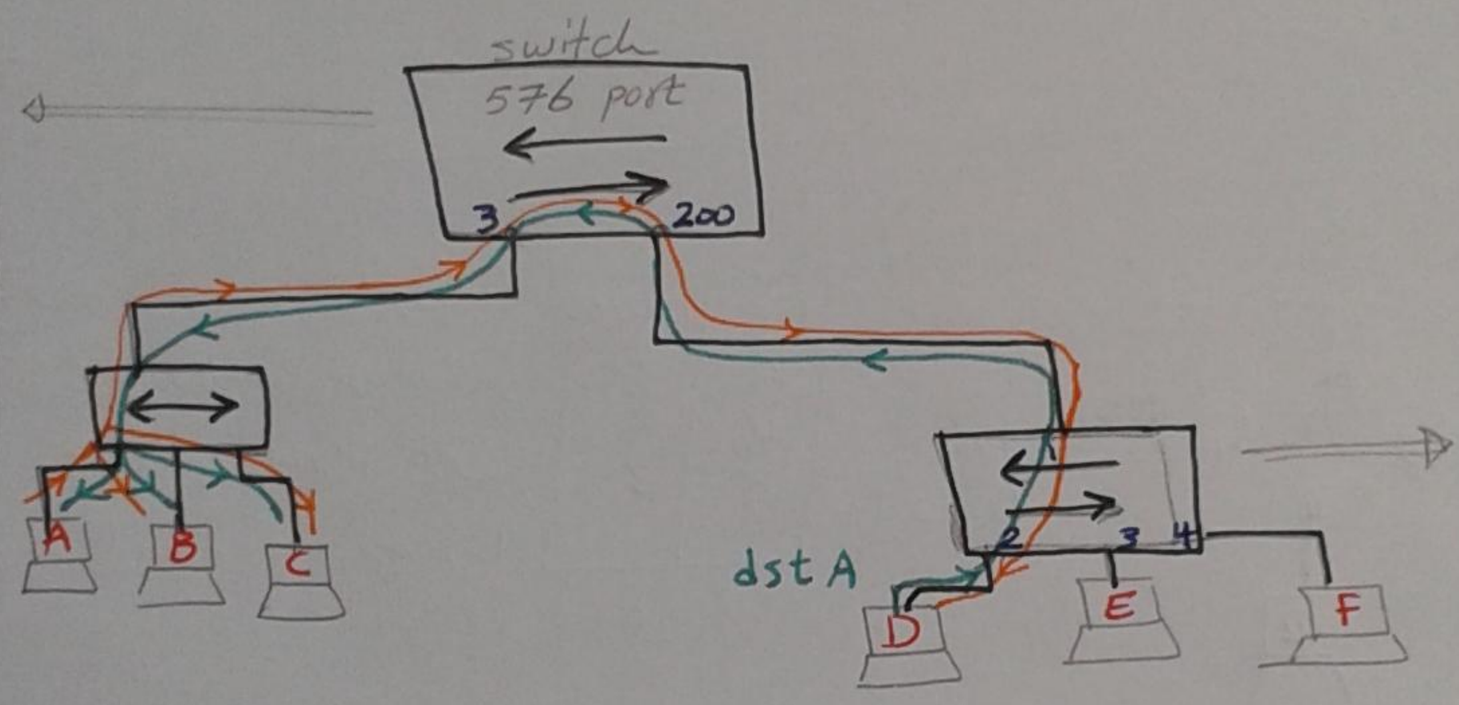


MAC Table

MAC	port
A	1
B	2
C	3
D	4

* the MAC table is in the volatile memory RAM

MAC	Port
A	3
B	3
C	3
D	200
E	200
F	200

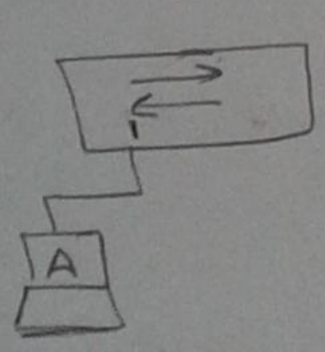


MAC	port
D	2
E	3
F	4
A	1
B	1
C	1

Note A switch can learn many devices on the same port

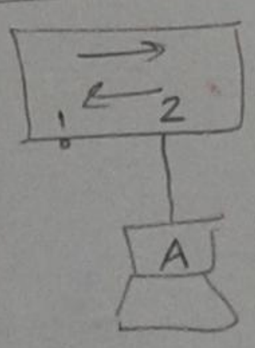
* switch flush (يمسح) inactive entries after 5 mins of inactivity by default
يعني انه لو الـ PC انفصل من الـ Network ← الـ Switch هيشيله من الجدول بعد 5 دقائق

NoteB switch will never learn existance of a device in 2 different ports



MAC	port
A	1

after a time



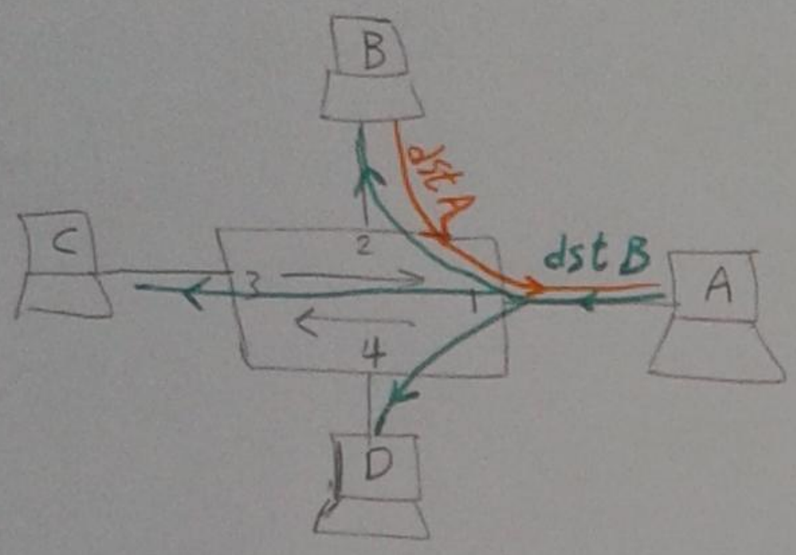
MAC	port
~~A~~	~~1~~
A	2

[2] forwording

switching frames to the next hop by checking dst MAC in any incoming frame

→ switch will flood If dst MAC :-

[1] If dst MAC is unknown unicast :-

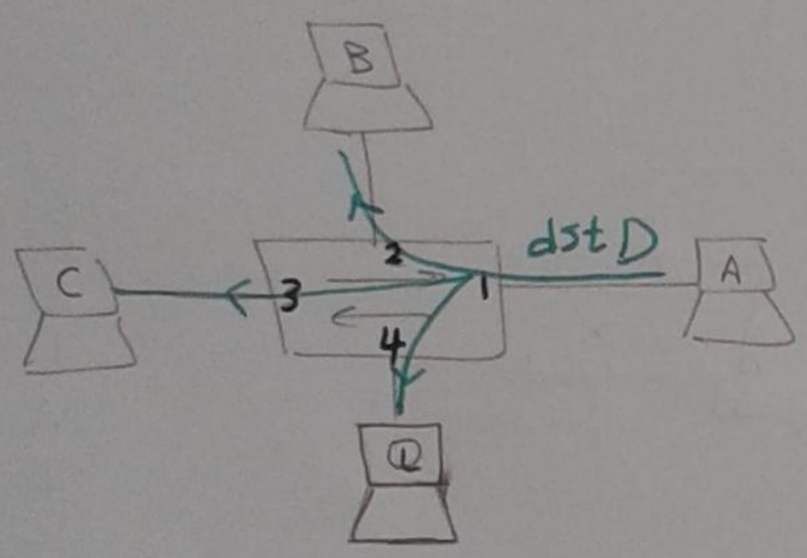


MAC	Port
A	1
B	2

في الحاله دى الـ switch هيعمل Flood و B بس هى اللى هتعمل process

[العمليه دى اسمها Handshating قبل ما يبعتوا لبعض]

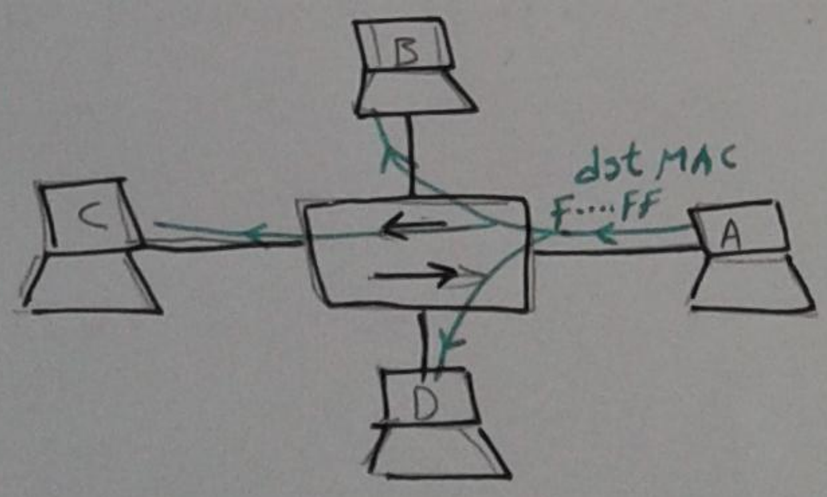
الـ switch بيـ Flood عشان يستنى الرد



MAC	port
A	1
B	2
C	3

لو الـ switch يعرف الجدول المقابل وبعدين A عايز يكلم D ⇐ في الحاله دى الـ switch تلزم بـ Flood على كل الـ ports عشان يوصل لجهاز D

[2] If dst MAC is Broad cast

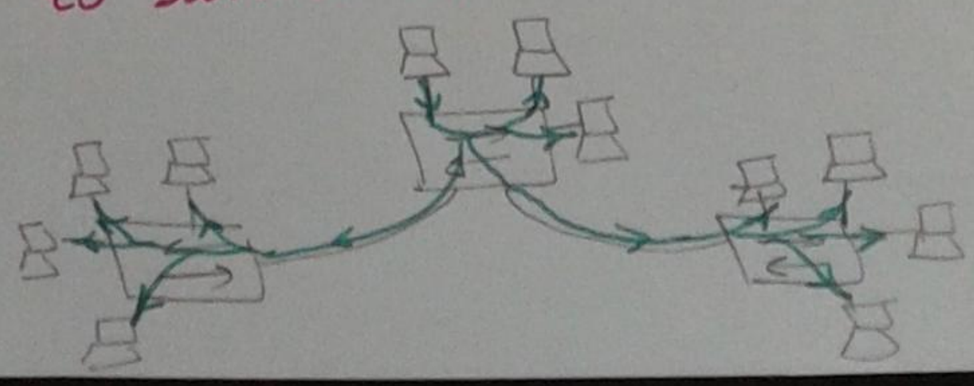


the switch doesn't broadcast [e.g Force the PCs to process the data] but the switch is Flood

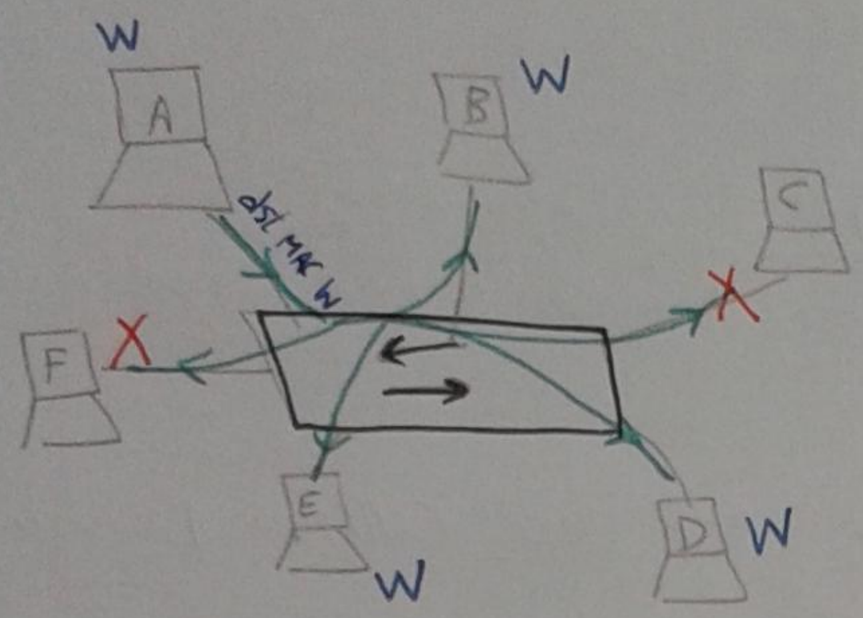
one Broad cast domain

Note < All devices connected to switch are members of a single Broadcast domain

This is also one broadcast DOmain



3] If dst MAC is multicast [it is used in Games]



* W ص ال dst بتاع ال Application

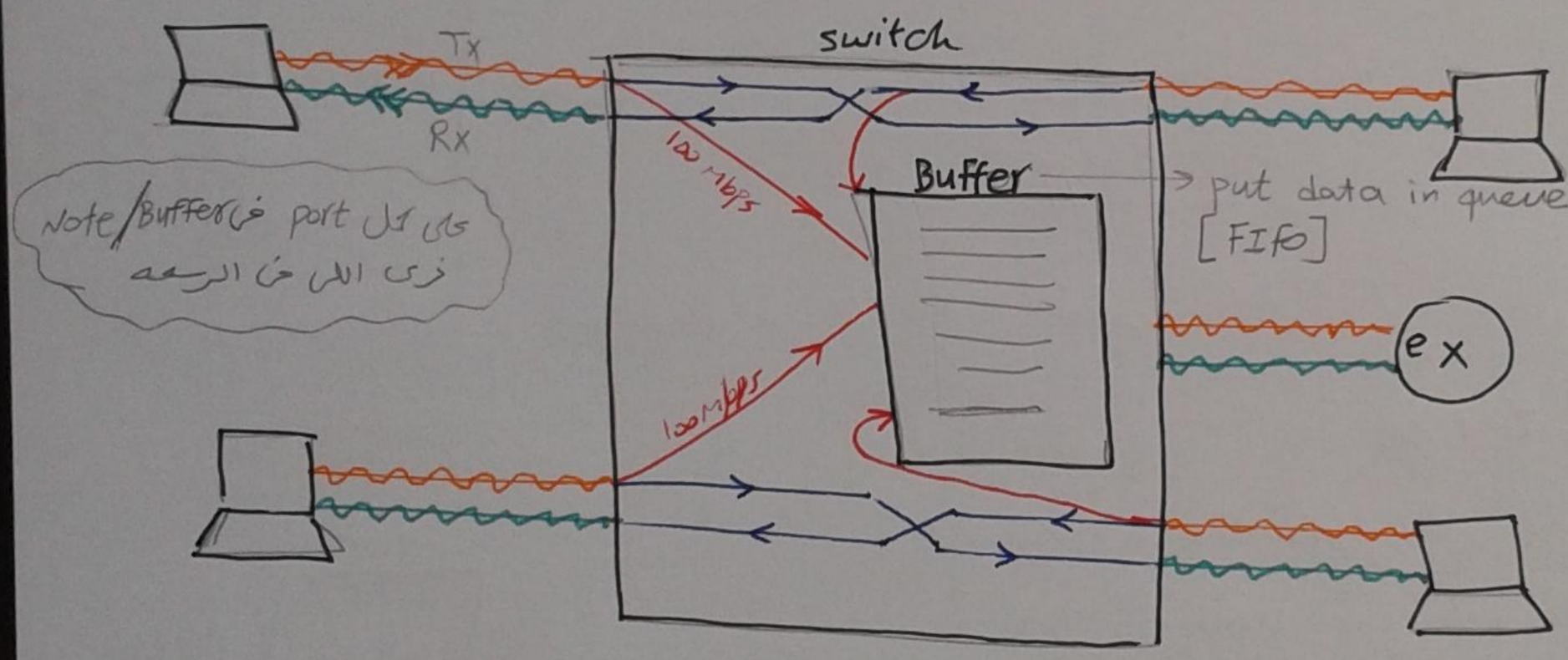
* ال switch بيـ Flood و اللى عايز يعمل process يعملها

XXXXX XXXXX
vendor Host

Multicast Appl ل ج/و

Note The main adv. of switch in Flood process that differ it from hub that there is no collission while Flood process

To avoid collision :- switch will forward using concept called Micro segmentation



Note D All devices connected to aswitch can operate in Full duplex [can both Tx & Rx at the same time]

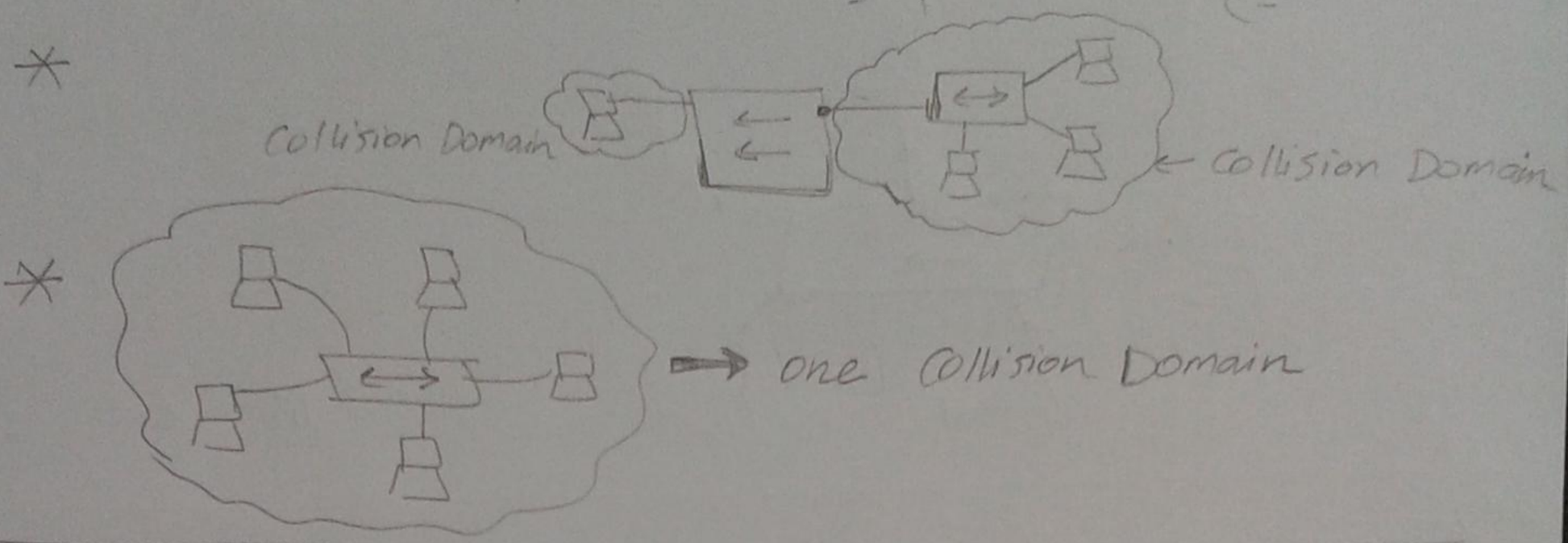
* لكنه ال Hub بيستخدم ال half duplex عن طريقه ال CSMA/CD

و الكمبيوتر هو اللى بيشغل ال CSMA/CD ⇐ هنا السؤال انه هل الكمبيوتر بيعرف انه اللى امامه switch ولا hub

⇐ الاجابه / ال PC بيبعت اشارة مش بيفهمها غير [layer2 device] ⇐ لو الاشارة رجعت لل PC هيفهم انه لاقى switch وهيلغى ال SCMA/CD ولو مرجعتش لل PC ~ ~ Hub وهيشغل ال SCMA/CD

Note E Each switch port is a separate collision domain

ای لا يتم تصادم بين ال ports وبعض



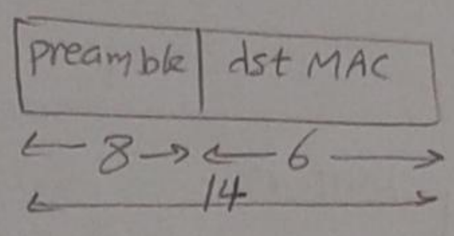
---

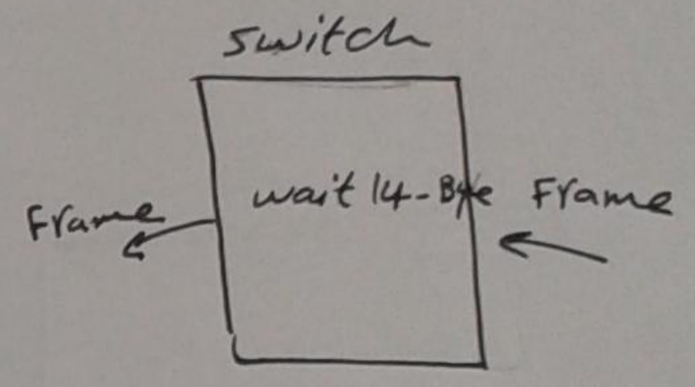
switch Forwarding modes (types) :— ≡ switching types

1 Cut through : سريع اوى لكنه بيعدى ال errors

wait after 14-byte then forward

↳ to check dst MAC





* بيستخدم ال switch ده في الشبكات الصغيرة فقط

---

2 Fragment Free (تنظيف)

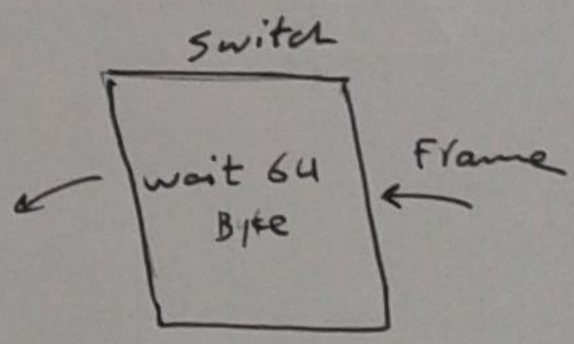
wait after 64-byte then forward

64-byte is the minimum Frame size

* بيستخدم ال switch ده لما يكون عندك في الشبكه Hubs

collision عشان يقدر يعرف ال wireless access point &

* مش بيعدى الا ال Frames النضيفه



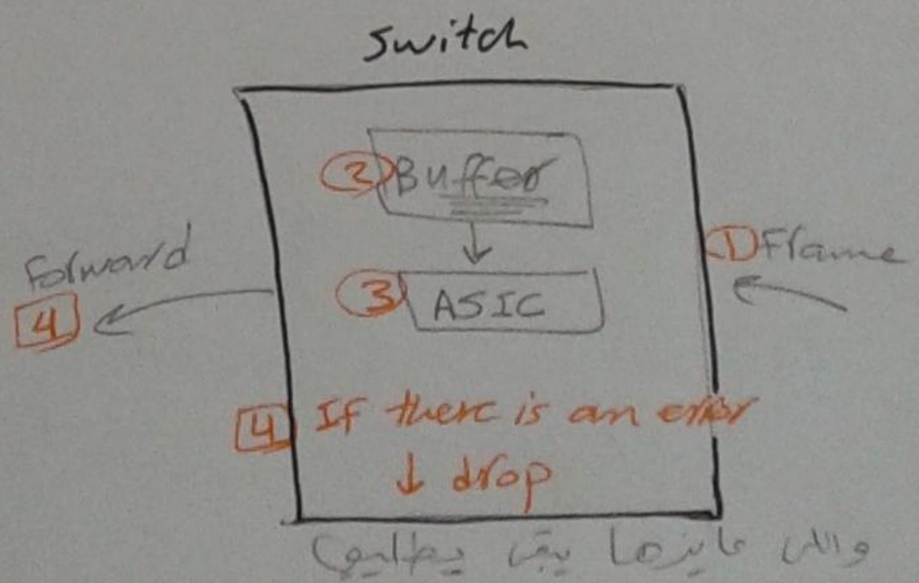
---

3 store & forward : عيبه انه بطئ

switch stores the full frame and check If there are any errors then forward

error types

- CRC errors
- Runt errors (Frame < 64 byte)
- Gaint errors (Frame > 1518 byte)



والى عايزها يفضل بطيئ

Store & Forward switch ⟹ Detect the error and drop it
it cannot correct the error
← بيعمل Check لكل ال Frames اللي بتمر عليه عشان كده هو بطيء أوي

---

[4] adaptive cut through : by Cisco

خليط من cut through و store & forward

starts as cut through untill the error Frames reaches a big no threshold, then changes to store & forward untill errors Frames reaches a small no, then return back to cut through

1. cut through If no errors
2. store Forward If high errors
3. cut through

Switch operation [continue]

1. learning
2. forwarding

[3] Remove L_2 loops :-

↓ STP (Spanning Tree protocol)

Rule for TCP/IP: each interface has L_2 and L_3 address
L_2 → MAC, L_3 → IP

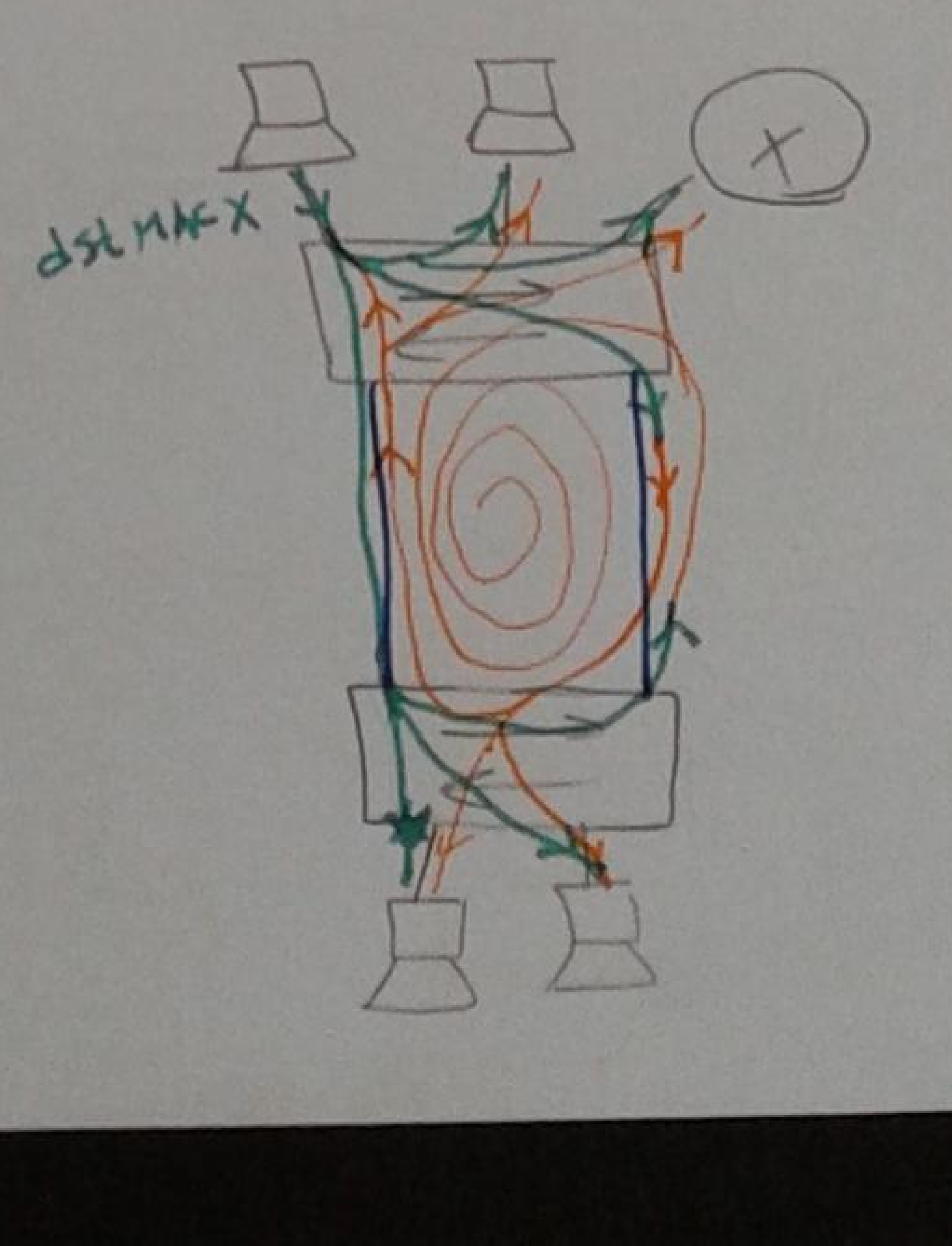
L_2 address →

-	Comm. Tech.	L_2 address (hop to hop address)
LAN	Ethernet wifi	MAC address MAC address
WAN	X.25	X.25 number
	Frame relay	DILC [Data link circuit ID]
	ATM	VPI / VCI vertual path ID / vertual circuit ID

L_2 address is address transport the data From Hop to Hop ⟹ one type of L_2 address is MAC

⟸ this table is some of L_2 addresses

we connect between the two switches by two wires (كابل) to sure redundancy



* المشكلة انك لو عملت Broadcast هيحصل Broadcast storm
* الحل في STP انه بيخلي كابل من الكابلين دول (stand by) link
يعني كأنه مش موجود ولو كابل اتقطع بيشغل الكابل التاني

* L3: Internet layer :- for end to end data delivary

it is responsible for

[1] logical addressing : Network part / Host part : S/W address

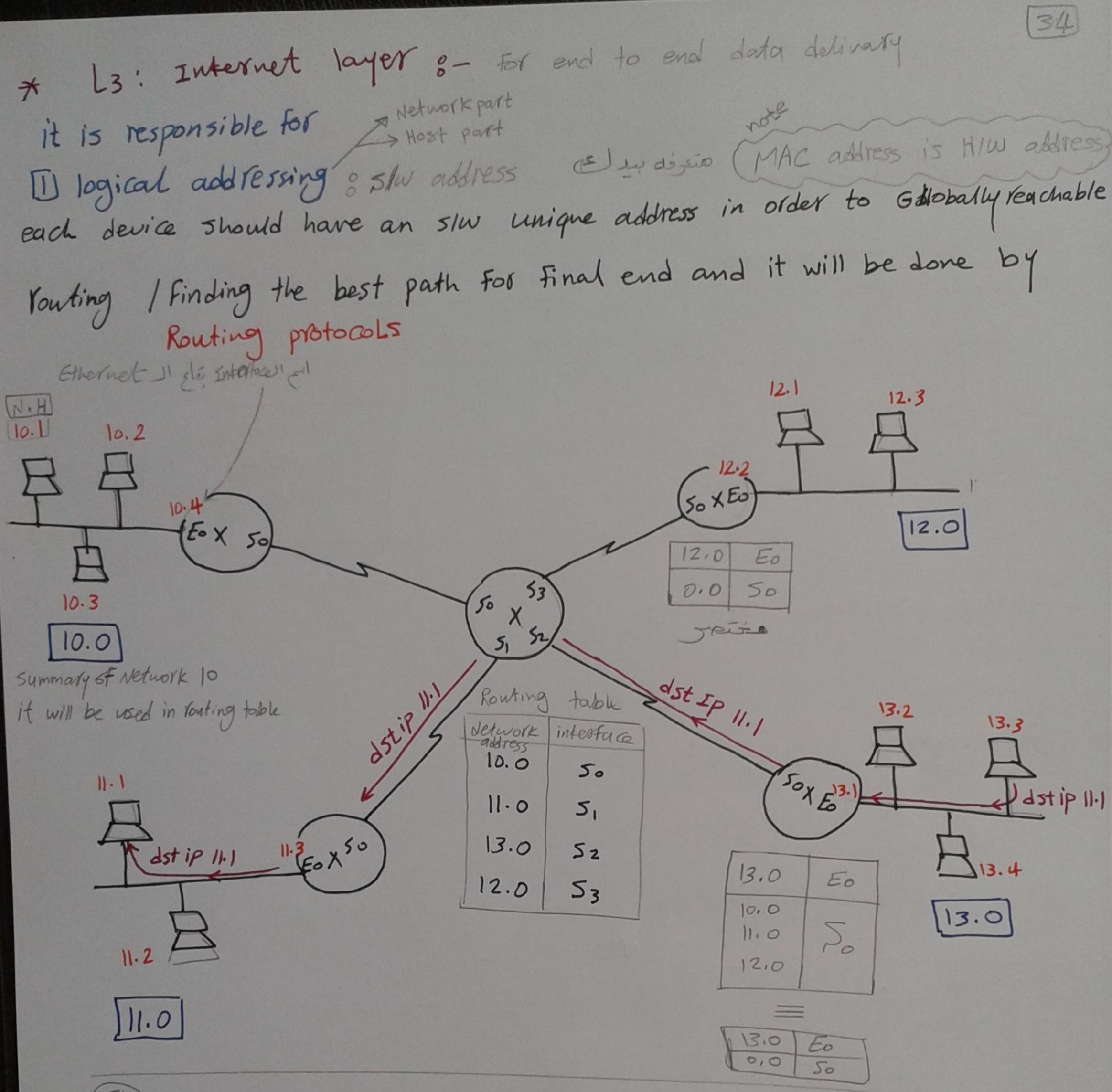
note: MAC address is H/W address متعرف بيدك

each device should have an S/W unique address in order to Globally reachable

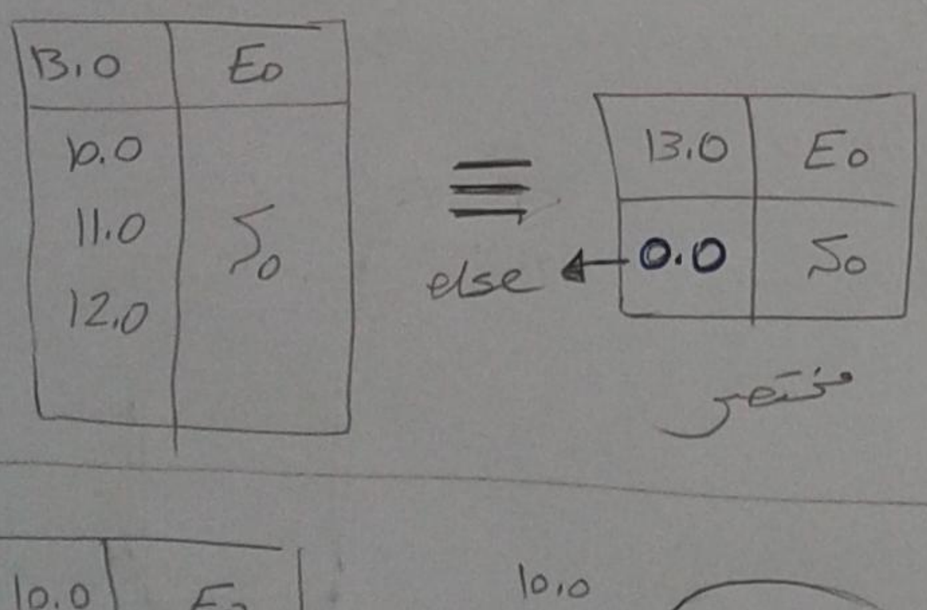
Routing / Finding the best path for final end and it will be done by

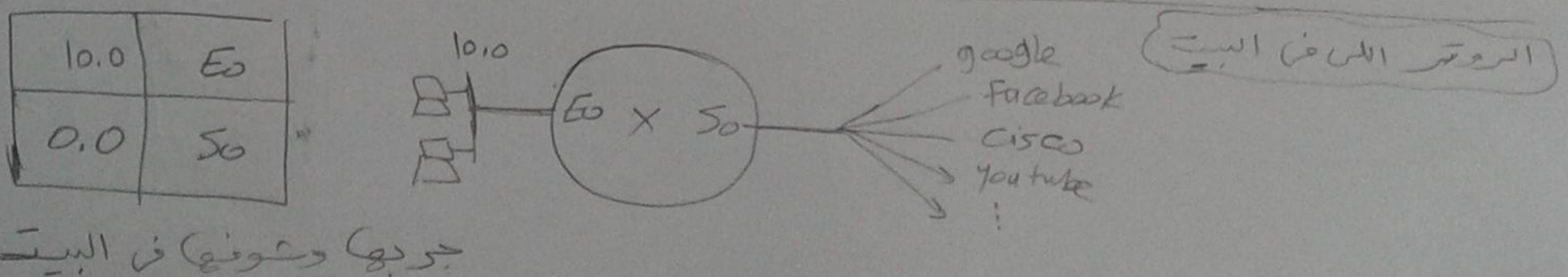
Routing protocols

Ethernet اسم الـ interface بتاع الـ



EX





switch operation

[1] Learn : Form MAC table by checking src MAC

[2] Forward : Compare dst MAC to MAC table

- If dst MAC is known ⟶ Forward
- ~ ~ ~ ~ unknown ⟶ Flood
- ~ ~ ~ ~ Broad cast ⟶ Flood

Router operation

[1] learn : By forming routing table formed by slw called Routing protocol

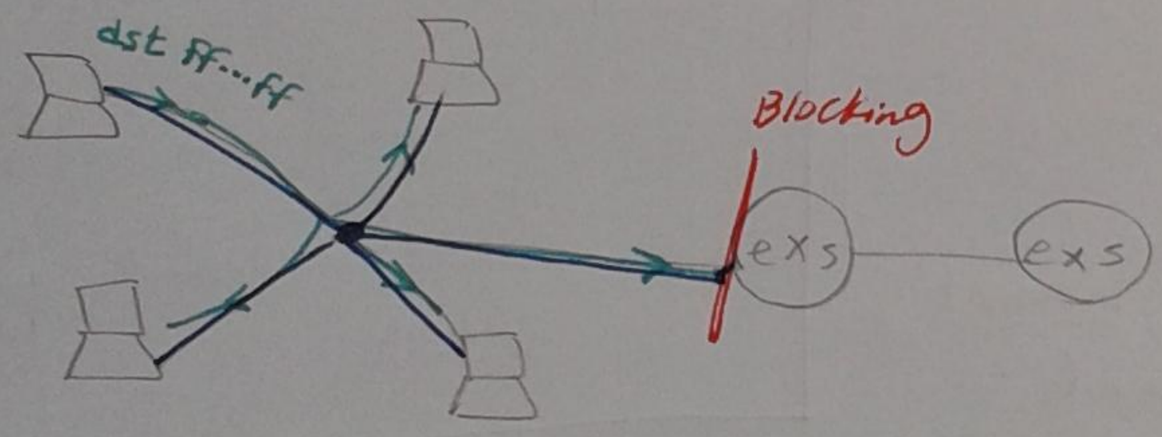
↳ ex : RIP$^{V_1}_{V_2}$, OSPF, BGP
IGRP, EIGRP, ISIS

[2] forward : By checking routing table

- If dst is known → Router will send the packet to the best path.
- If dst is unknown → Router will drop data

* Router should learn before forwarding

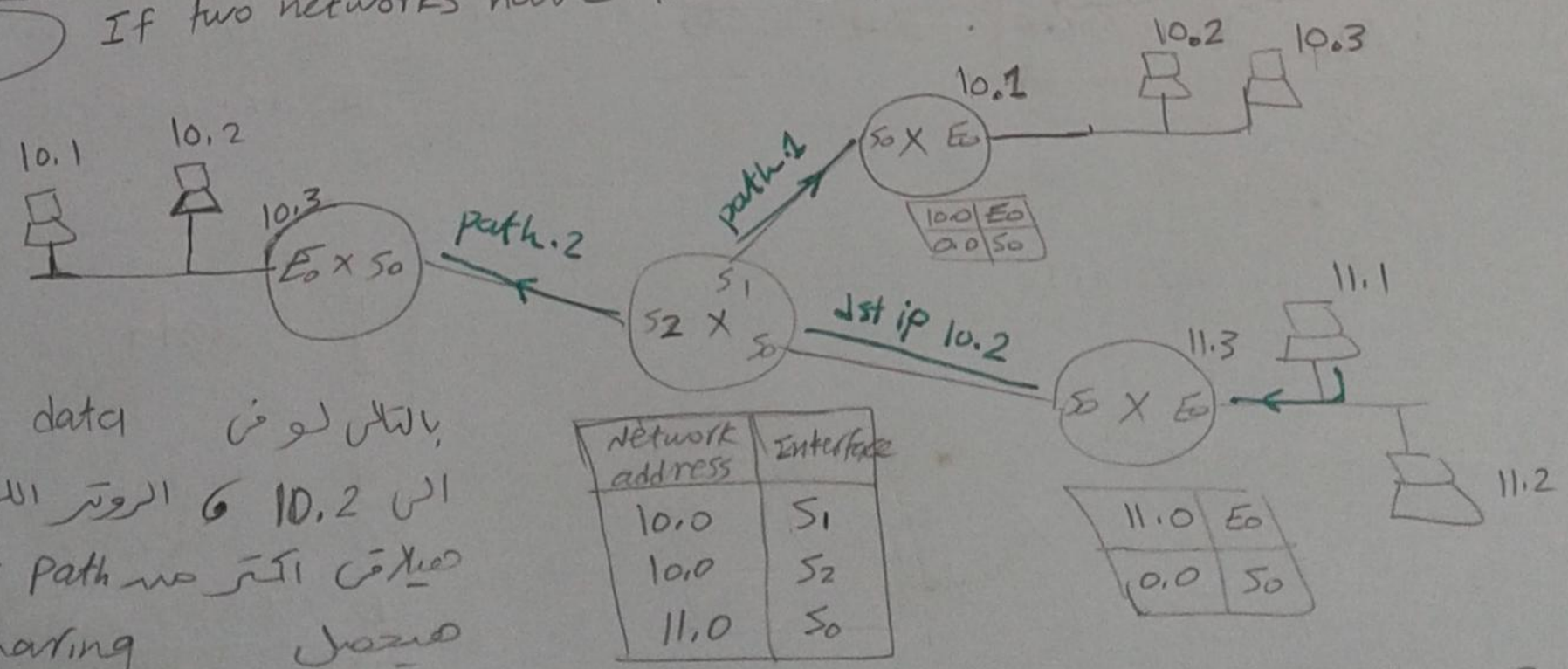
- If dst is Broadcast → Router will take packet to itself



* The router make Blocking of Broadcast and doesn't pass the data behined itself

---

note If two networks have the same name 10.0



11.1 من جاية data بالتالي لو فى
الى 10.2 و الروتر اللى فى النص
صيلاقى اكتر من best path وبالتالى
صيعمل
- load sharing
- load Balancing ⟶ send packed on path 1 & next packet to path 2 & so on
والدنيا مضبوط

* layer 3 protocols :-

ex: IP V4 : internet protocol

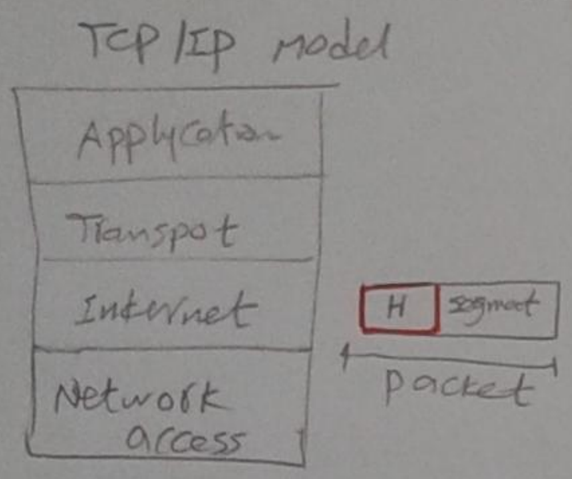
responsible for :-
- logical addressing by using IPv4 address
- end to end encapsulation [delivery] ⟶ IP V4 packet

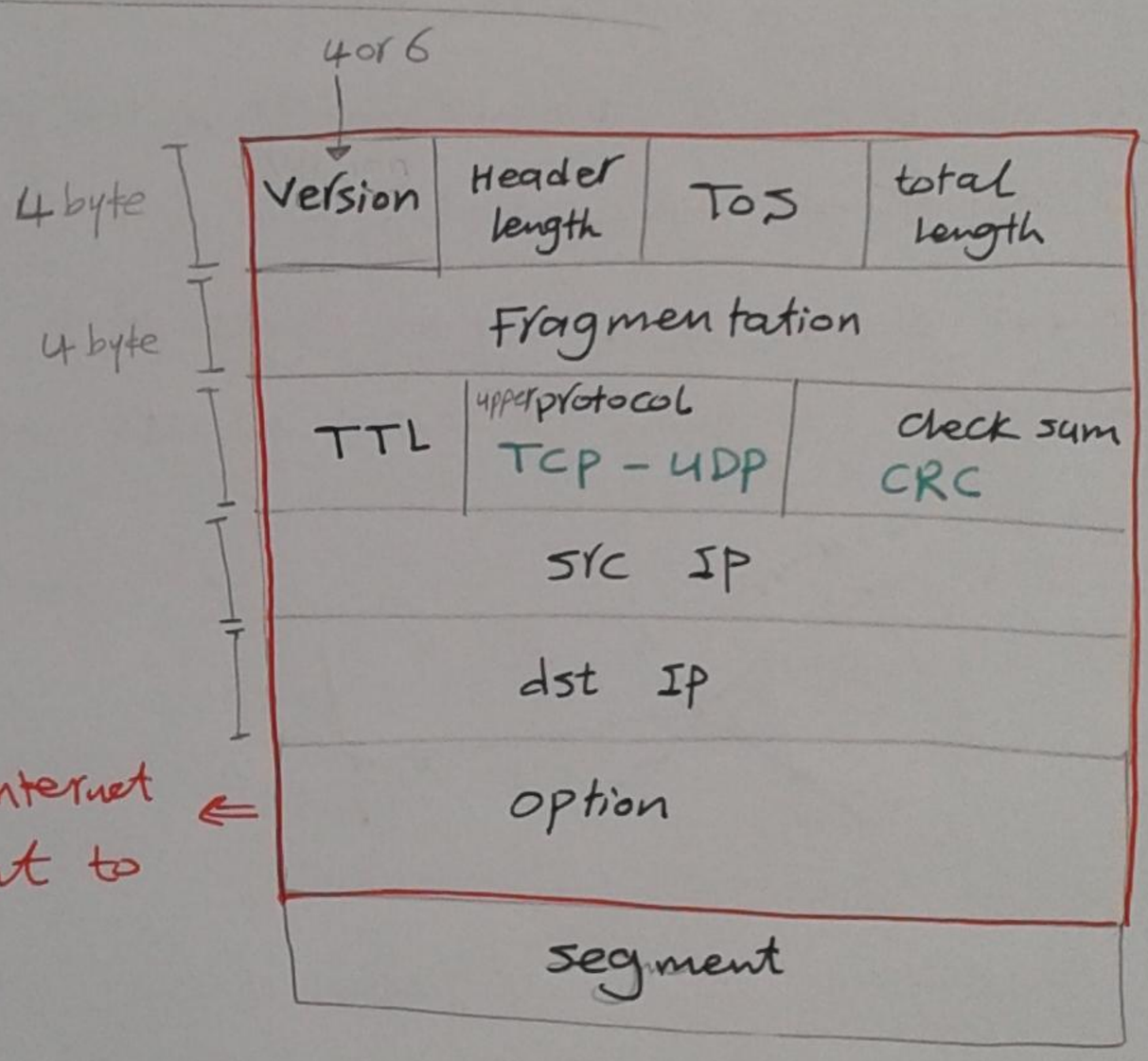
IP V4 addressing ⟶ 32-bit represented in dotted decimal

10101010 . 11110000 . 10111001 . 10111111

8bit ≡ byte ≡ octet

ex : 170.20.5.192

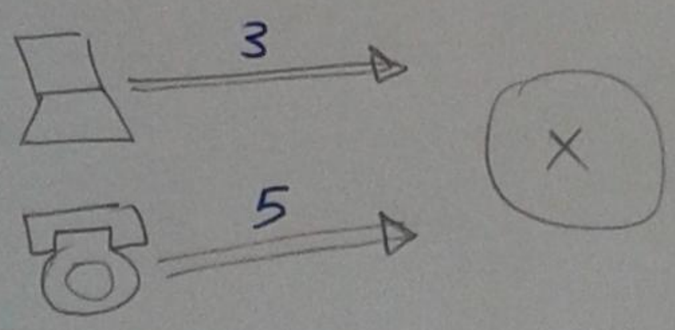




This is the header that internet layer add to the segment to form the packet

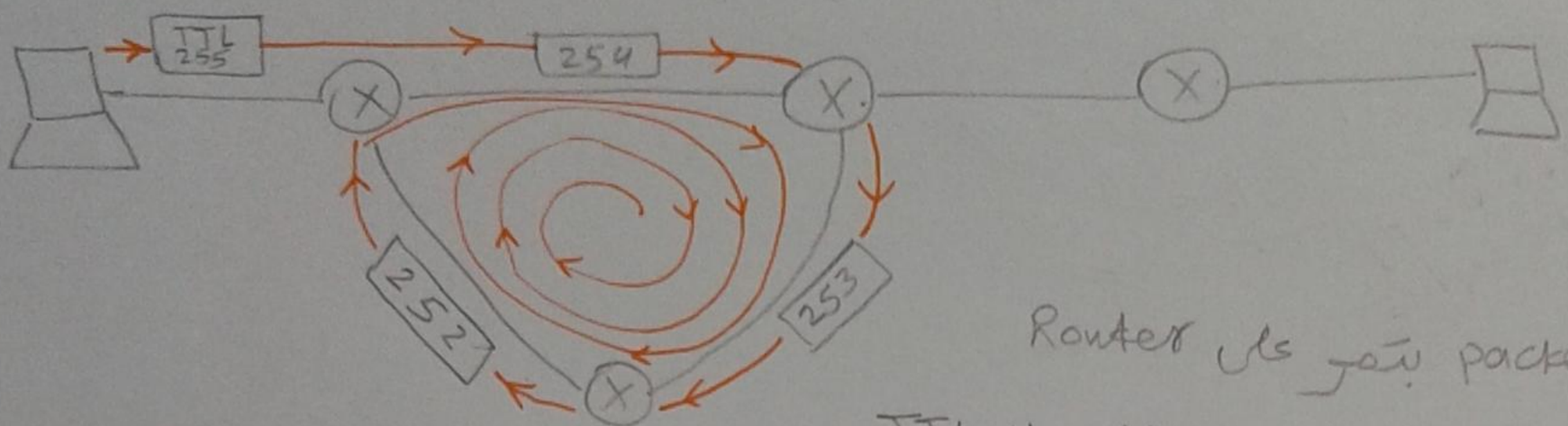
* TOS : type of service ⟶ reflect periority [the highest the number the highest the perority]

it is 3 bits → 0 000, 1 001, ... 7 111



0 1 2 3	data
4	vedio
5	voice
6	Router protocol
7	switch protocol

TTL : time to live it is 8 bits [0—255]



* كل ما الـ packet بتعدي على Router
← الـ Router هينقص 1 من خانه الـ TTL
* لو الـ Router شاف الداتا في خانه الـ TTL = 1 ⇐ هيعرف انه الـ Data دي بتعمل loop بقالها فترة كبيرة قدرها 254 مرة وهياخد القرار انه يرميها
⇐ العمليه دي بتحصل لأن في الحقيقه عشان توصل لأي Router في العالم بتعمل عدد hops قليله لا تتعدى 20 hop على 20 Router حول العالم

---

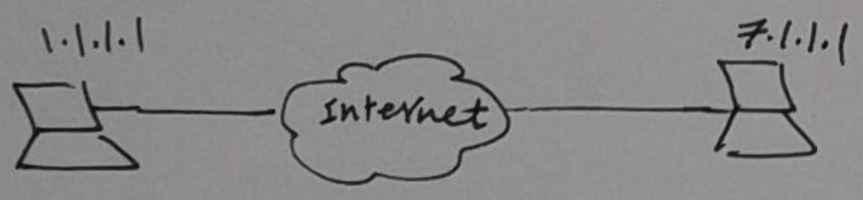
* ازاي تعمل Check على end to end عشان تتأكد انه الـ Data بتروح من end الى end

* Troubshooting protocol from end to end

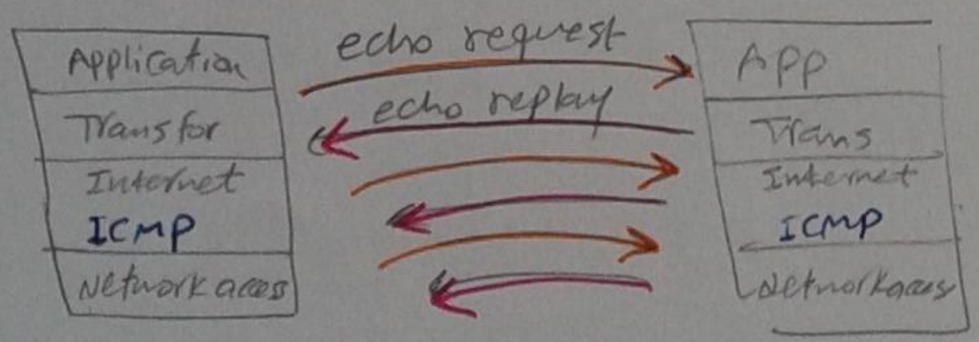
ICMP [internet control Messaging protocol] موجود في Internet layer
يعالج مشاكل — using message

البروتوكول ده شغلته انه يبعت رسايل للـ end ولو رجعت الرساله يبقى الدنيا شغاله

[1] echo request & echo replay Msg :-



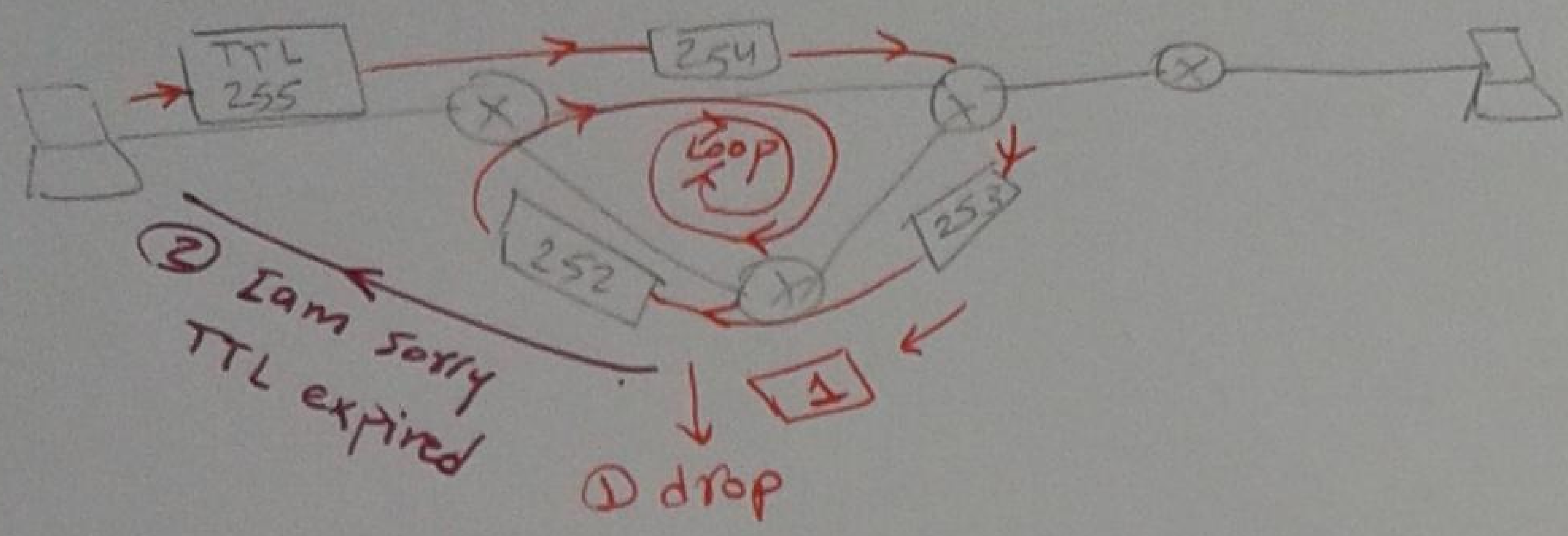
افترض انك على جهاز 1.1.1.1 و عايز تبعت request للجهاز 7.1.1.1 عشان تتأكد انه شغال وهيقدر يتواصل معاك
فهتعمل Command بسيط اسمه ping 7.1.1.1
لو 7.1.1.1 شغال هيبعت رد عليك وبالتالي انت هتعرف انه شغال



بيعمل
windows → 4 echo
IOS → 5 echo
linux → ∞ echo

* بعد ما بتعمل امر ping 7.1.1.1 ⇐ الـ PC بيقولك الـ Data بتروح وتيجي بمعدل 100%

[2] TTL expiration message



الامر → PC → Start → Run → CMd → Trace www.fB.com
على الـ DOS

ping www.fB.com ملحوظة انت ممكن تعمل

Session 8

- الهيئة المسؤله عن توزيع الـ IPs اسمها IANA

IPv4 classes :-

[1] Class A N. H. H. H (Fixed: N; Variable: H.H.H)

First octet : 1 → 126

(EX) 57.X.X.X
57.0.0.0 (Network address) — summary of some devices
57.255.255.255 (direct Broad cast) — used for appl. & protocol
These two IPs don't be used as IPs for end devices

[2] Class B N.N.H.H

First octet : 128 → 191

[3] Class C N.N.N.H

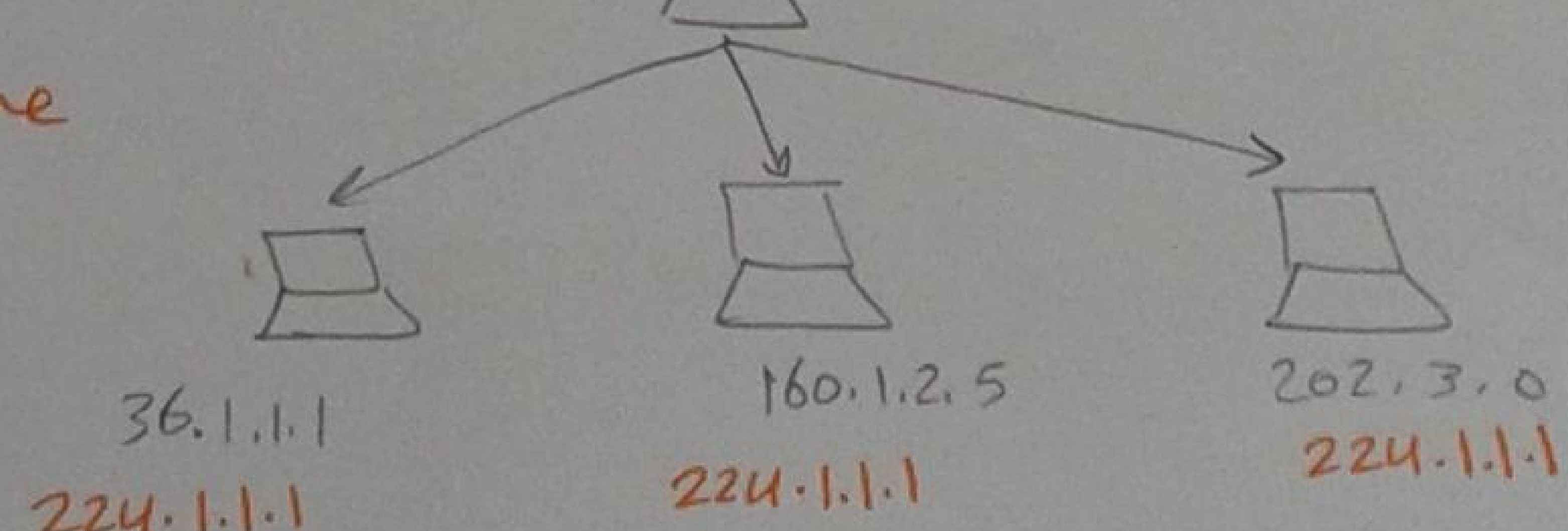
First octet : 192 → 223

(Note) Each interface [DTE] should have either Class A or B or C address

[4] class D reserved for Multicast application

First octet : 224 → 239

(244.1.1.1) is Extra address that the application give to you ← this is vertual IP
⇒ this IP is burnt in the RAM
* الـ IEEE بيعطى MAC لكل الاجهزة اكمان

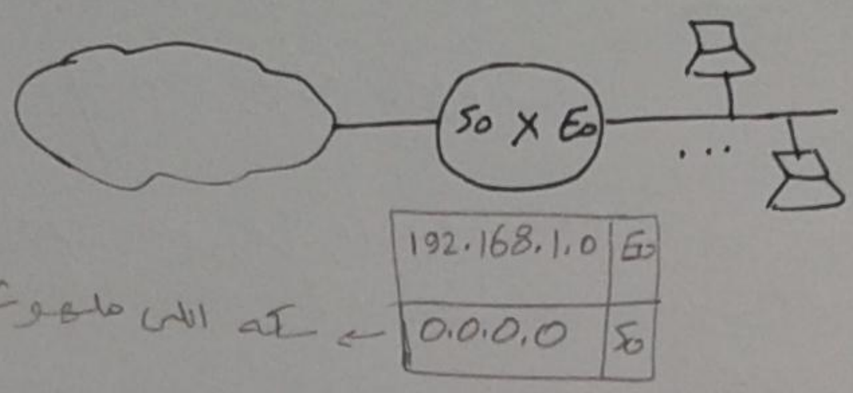


Class E : used for Experements and recearches

First octet : 240 — 254

Classless IPs :-

[A] 0.0.0.0 - it is the sammary of all networks [IPv4 Networks]
- it is used in routers tables



← كله اللى جاوشى بكله

[B] 127 → used for loopback test [self test] ⇒ يعنى لو عايز تـ Test الروتر او ال pc بتاعك

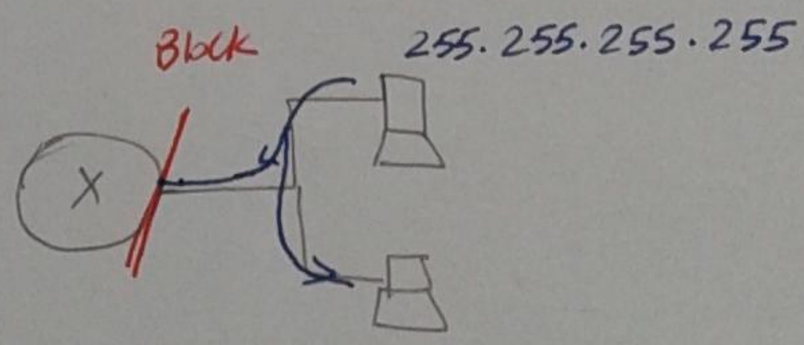
127.0.0.1 used for TCP/IP test ⇒ عشان تتأكد انه ال TCP/IP بتاع الجهاز بتاعك شغال

Command on the DOS ⇒ ping 127.0.0.1

[C] 255.255.255.255

- Local Broad cast

كل كارت من كروت ال Network بيقى فيه unicast Ip خاص بالكارت + الـ Ip بتاع



255.255.255.255 → non Routing

57.255.255.255 → Routable

هنا الـ Router بيعمله process ومش بيعدى بعدة

used for applications and protocols

* Classifaction of IPs

EX.1 57.0.0.0 [Network address] e.g {summary of some devices}

57.0.0.1
⋮
57.255.255.254

Hosts = $2^{24} - 2$
no of IPs = 2^{24}
no of hosts = $2^{24} - 2$

57.255.255.255 ⟹ it is used for App & protocols for Network 57 only

بس 57 دة عنوان كل الاجهزة اللى فى Network اللى عنوانها
يعنى لو فى شبكه عنوانها 63 مثلا و مش هتستقبل العنوان دة

255.255.255.255 ⟶ دة عنوان كل الاجهزة فى العالم

EX.2 191.16.X.X

191.16.0.0 ⟹ Network address [summary of this Network]
191.16.255.255 ⟹ direct broadcast

no of IPs = 2^{16}
no of Hosts = $2^{16} - 2$

EX.3 192.168.1.X

192.168.1.0 ⟹ Network address
192.168.1.255 ⟹ direct address

no of IPs = 2^8
no of hosts = $2^8 - 2$

* IP V4 Shortage :-

Network need IPV4	Class ??	wasted IPs ??
6	class C [256 IP]	250 IPs
536	class B [65536]	65000 IP
300,000	class A [16,xxx,xxx]	16,xxx,xxx

* solutions :-

1. IP V5 : 64 bit address
2. IP V6 : 128 bit address $\simeq 5 * 10^{28}$ IPV6 / human

---

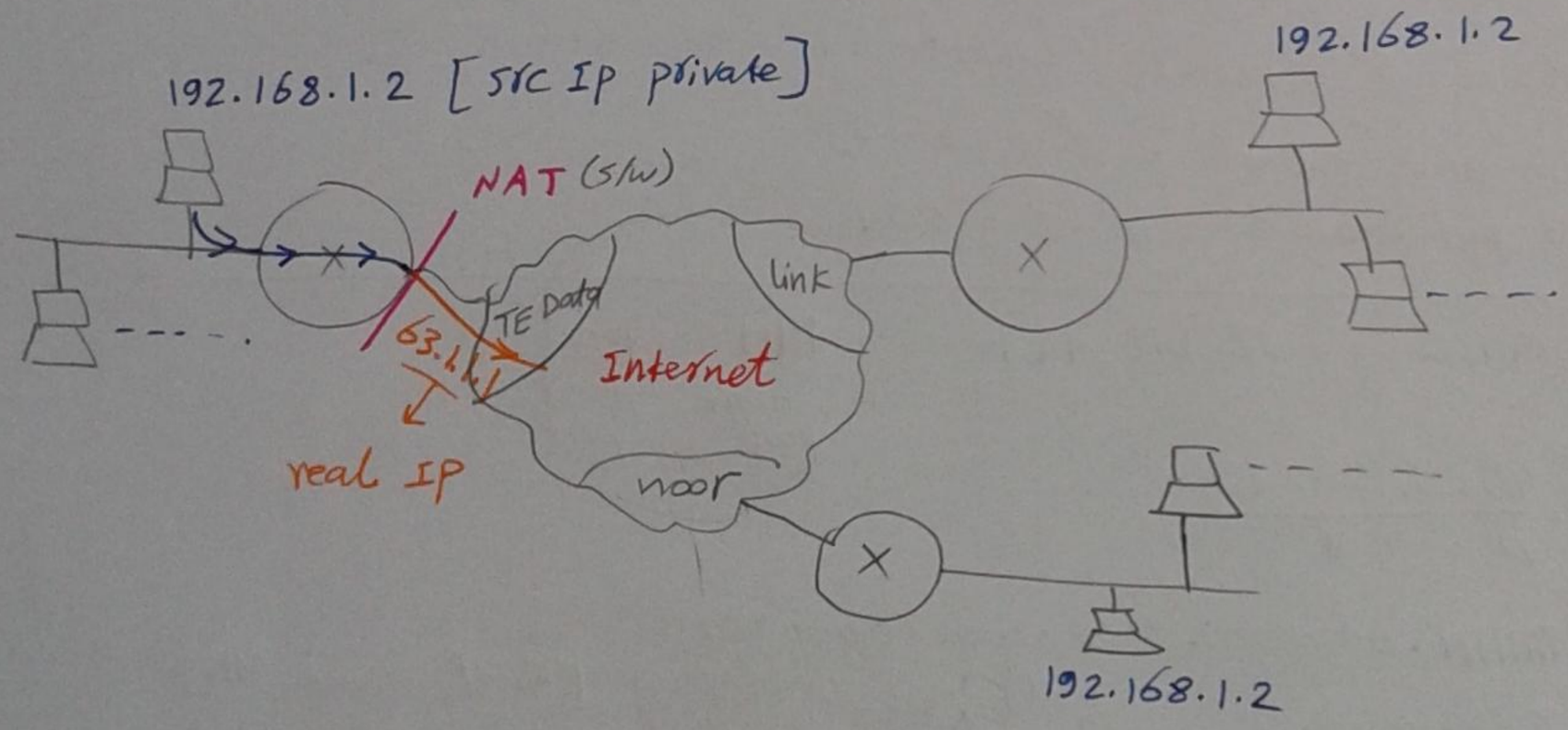
* private IPs + NAT (Network address Translation)

* any one can use the following IPs without registeration but For private use only

10.X.X.X

172.16.X.X ⟶ 172.31.X.X

192.168.0.X ⟶ 192.168.255.X



NAT ⇐ S/W بيحول الـ private IP الى public IP

بيقدر اكتر من private IP يشيّروا ف one public IP

Subnetworking: it is deviding Major network in to smaller networks called subnets

* subneting is done by borrowing part of Host bits & give them to network part

200.1.1.0 } Subnet 1
200.1.1.7 }
200.1.1.8 } subnet2
200.1.1.15 }

* نفترض هنا ان كل الـ subnets متساوية في الحجم

ex.1

57.X.X.X
N | SN=8 | H=16

57.0.X.X 57.1.X.X 57.2.X.X 57.255.X.X

no of subnets = $2^{SN} = 2^8 = 256$ subnets

no of IPs in one subnet = $2^H = 2^{16} = 65536$

ex.2

58.X.X.X
N | SN=16 | H=8

58.0.0.X 58.0.1.X 58.0.2.X 58.0.255.X 58.1.0.X 58.255.255.X

no of subnets = $2^{16} = 65536$ subnets

no of IPs in one subnet = $2^8 = 256$ IP

no of Hosts per subnet = $2^8 - 2 = 254$

* subnet Mask 32-bit Mask 11111---0000
Network part | Host part

ex.1 IP: 63.5.70.120
N | H

Mask: 11111111.00000000.0000 0000.00000000

255.0.0.0 or /8 ← عدد الواحدات في الـ Mask [no of Network bits]

ex.2 IP: 128.50.3.200
N | H

MASK: 11111111.11111111.00000000.00000000

255.255.0.0 or /16

Ex·3

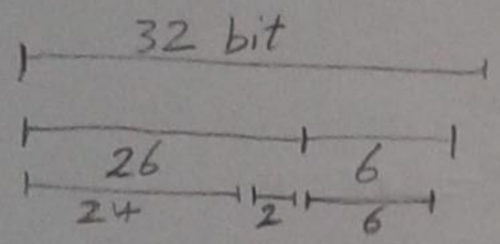
200.1.1.X /24

XX XXXXXX
SN H

subnet 1	subnet 2 (N)	subnet 3	subnet 4
200.1.1.00000000	200.1.1.01000000	200.1.1.10000000	200.1.1.11000000
200.1.1.00000001	200.1.1.01000001	200.1.1.10000001	200.1.1.11000001
200.1.1.00000010	200.1.1.01000010	200.1.1.10000010	200.1.1.11000010
⋮	⋮	⋮	⋮
200.1.1.00111111	200.1.1.01111111	200.1.1.10111111	200.1.1.11111111
the subnet address	the subnet address	the subnet address	the subnet address
200.1.1.0 /26	200.1.1.64 /26	200.1.1.128 /26	200.1.1.192/26
direct Broad cast address	direct Broad cast address	direct Broad cast address	direct broad cast address
200.1.1.63 /26	200.1.1.127 /26	200.1.1.191 /26	200.1.1.255 /26

FATAKA Method

/26



No of subnets = $2^2 = 4$

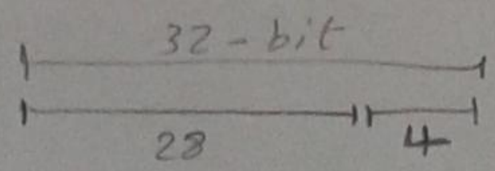
No of IPs /subnet = $2^6 = 64$ ← the step

	subnet 1	subnet 2	subnet 3	subct 3
Start	200.1.1.0 /26	200.1.1.64/26	200.1.1.128/26	200.1.1.192/26
end	200.1.1.63/26	200.1.1.127/26	200.1.1.191/26	200.1.1.255/26

Ex.1 For the major network 193.168.5.0/24 , Devide it into 16 subnet each contain 16 IP

Sol: No of subnet = $16 = 2^4$ ∴ new network = 24 + 4 = 28 bit

no of IPs = 16 ∴ new host part = 4 bit



1st subnet address → 193.168.5.0/28 → اخر IP بتاعه تجيب الـ Direct BRoadcast address

2nd ~ ~ → 193.168.5.16 /28

3rd ~ ~ → 193.168.5.32 /28

4rth ~ ~ → 193.168.5.48 /28

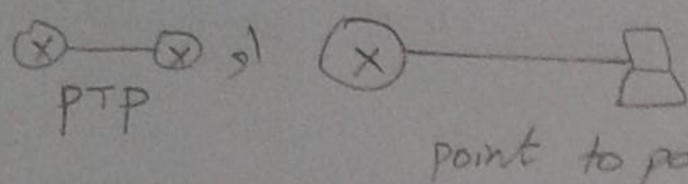
5th ~ ~ → 193.168.5.64/28

⋮ ⋮

last ~ ~ ~ → 193.168.5.255 /28

EX.2 * Find the largest Mask ???

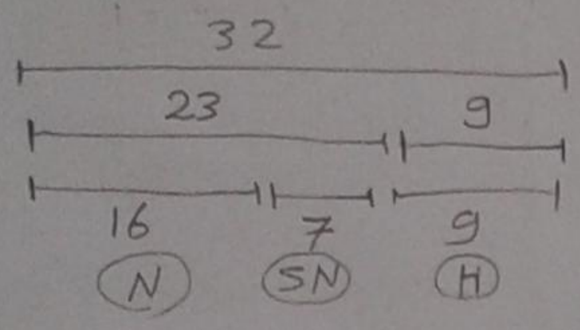
⟹ /30 ⟨ N = 30
H = 2 ⟹ No of IPs = $2^2 = 4$
No of Hosts = 4 - 2 = 2



⟸ بس هي اصغر Network ممكن اعملها في حياتي

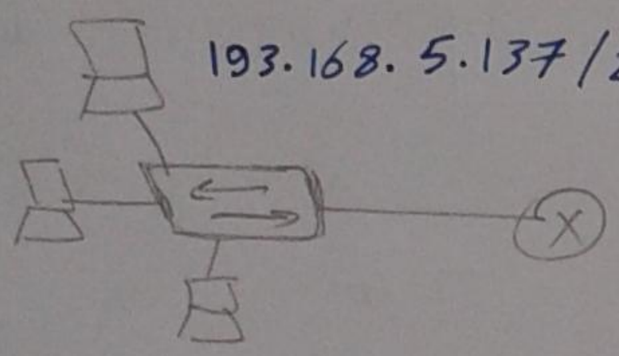
The Mask for this Network = 255.255.255.252 ⟹ ≡ /30
Mask يبقى ده الـ

EX.3 127.16.0.0/16 Devide it to /23



∴ No of subnets = 2^7 = 128
No of IPs = 2^9 = 512
No of Hosts = 510

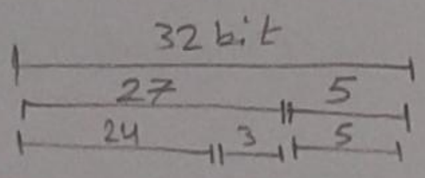
EX.4



find
- subnetwork address
- Direct Broadcast address
- valid IPs for Hosts

Sol.

1 FATAKA method



no of subnets = 2^3 = 8
no of IPs = 2^5 = 32 IP
no of Hosts = 30

193.168.5.0/24

193.168.5.0/27
193.168.5.32/27
193.168.5.128/27
193.168.5.160/32
subnet address
193.168.5.137/27
Direct Broad cast address
193.168.5.159/27

الطريقة دي ممكن يكون فيها قصور لو وجد اكتر من Subnets اوي

⟹ Solution FATAKA AWY Method

IP : 193.168.5.137/27

IP : 193.168.5.10001001
N = 27 H = 5

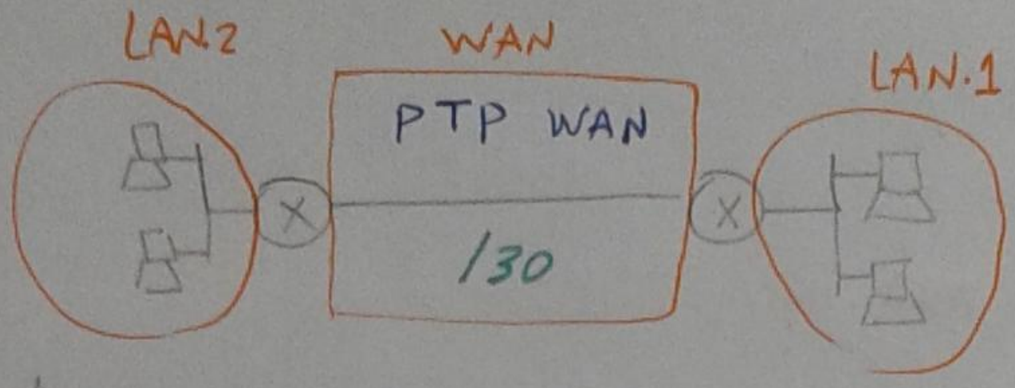
193.168.5.100 00000 = 193.168.5.128 [subnet address]
193.168.5.100 11111 = 193.168.5.159 [direct Broadcast address]

Binary الى 137 تحويل او

137
- 128 → 128
9
- 8 → 8
1
- 1 → 1
0

137 = 10001001

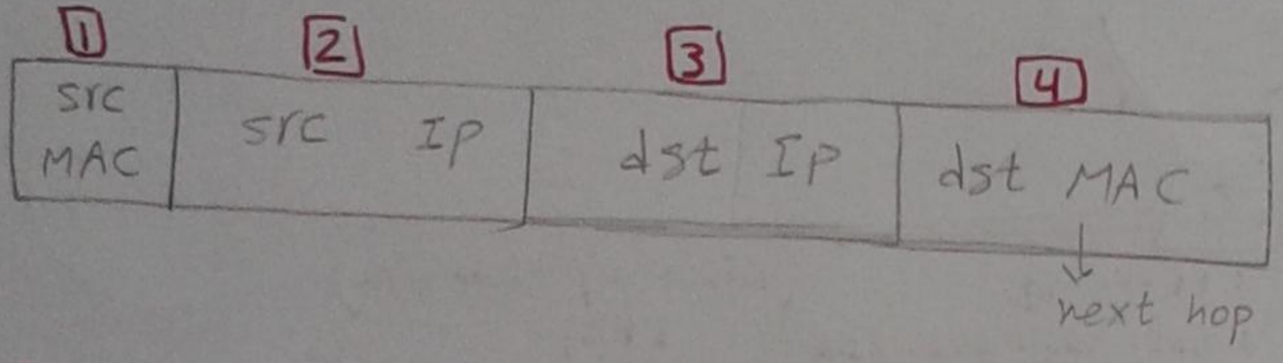
IQ technical



there are 3 networks not 2

Session 10

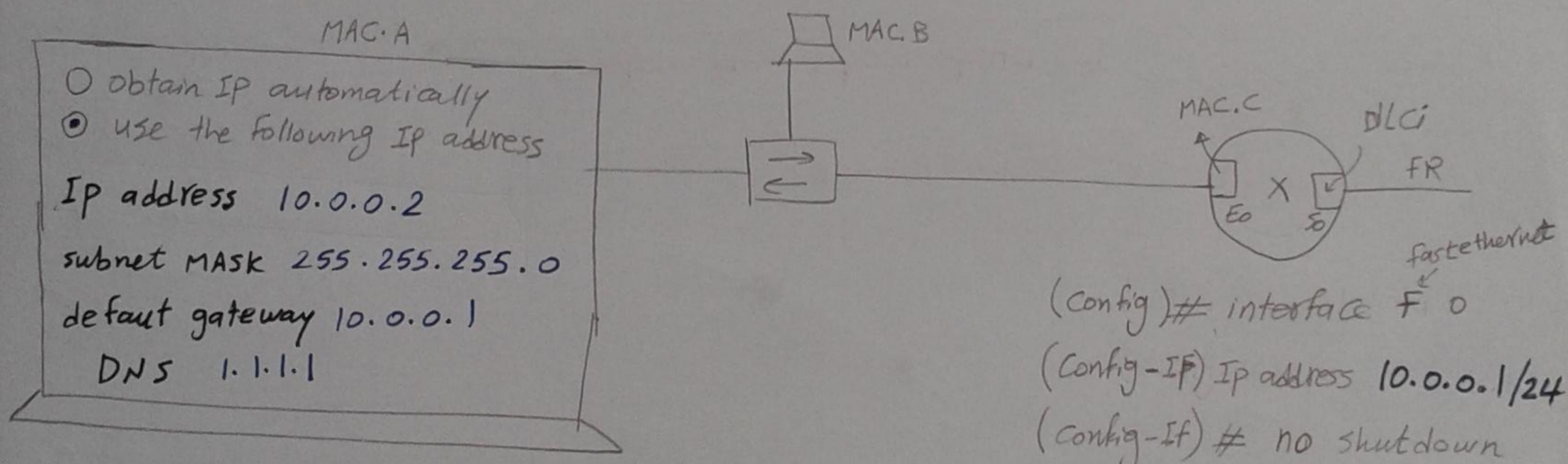
Getting started For end to end data delivery



1 src MAC : it is burnt on Rom of NIC [Network interface card]

2 src IP

A manually [you give it to DTEs]



منا اديت اعطيت للروتر IP

1 Ip address 10.0.0.2
2 subnet Mask 255.255.255.0 ← الامرين دول ال PC يقدر من خلالهم يتكلم LAN فقط

3 default gateway 10.0.0.1 ← الامر ده ، ال PC يقدر من خلاله يتكلم WAN مع شبكات اخرى

4 DNS 1.1.1.1 ← من خلال الامر ده ال PC يقدر يدخل على ال Internet

B automatically

* الـ PCs بتاخد الـ unicast IP من تلات servers & protocol

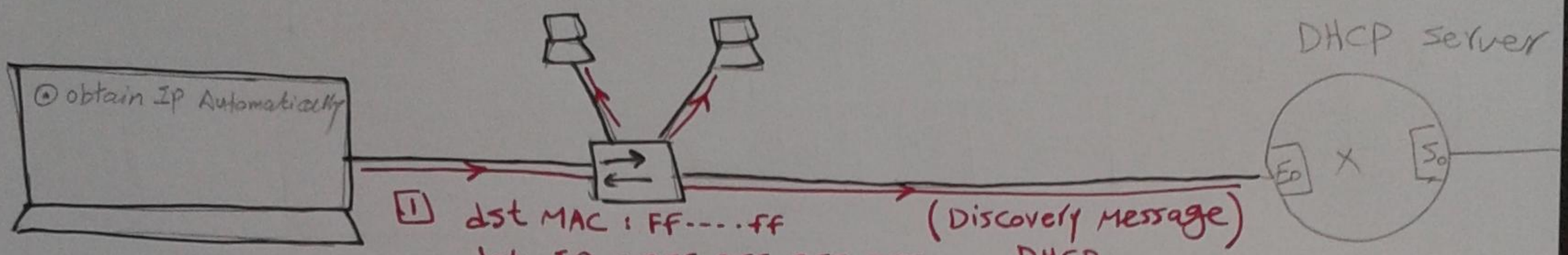
* أنواع الـ protocols اللى بيستخدموا العملية دى

1 - RARP (old) (revere ARP)

2 - Boot P (old) (Booting protocol)

3 - DHCP (New) (Dynamic Host Configiration protocol) ← دة اللى بيستخدم حاليا

↳ this protocol exist in layer 7



لو الـ PC موافقه يأخد الـ IP ده هيقول للـ server احجزهالى

موافقه

* فى بعض الشركات بتعمل 2 servers عشان يخدموا الـ PCs ويوفروا وقت فى اعطاء IPs للـ PCs

لو الـ PC بعت رساله للـ 2server و الـ 2server ردوا عليه و الـ PC هيعمل accept على اسرع offer وش هيقدر يشتغل بالـ IP ده الا لما يجيله ack من الـ server

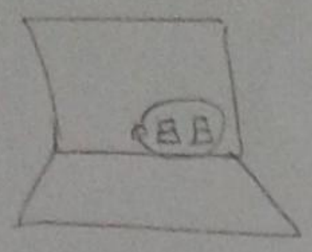
---

فى Interview هيرخم عليك ويقولك ازاى الـ Router يكون L3 ويشغل DHCP اللى هو L7

← بدل ما اشترى server ← انزل S/W (DHCP) على الروتر وهو هيقوم بعمل الـ server و يوزع IPs وهنا الروتر عمل وظيفه واحده بس من L7

وممكن كمان الروتر يعمل Telnet

اثناء تنفيذ الـ ٤ خطوات اللى فاتوا بتظهر الصوره دى



مرحله بحث

العمليه نجحت والـ PC حصل على IP ← نجاح

فشل

* the defaut of Automatic Ip is Dynamic , but you can change it to static Ip

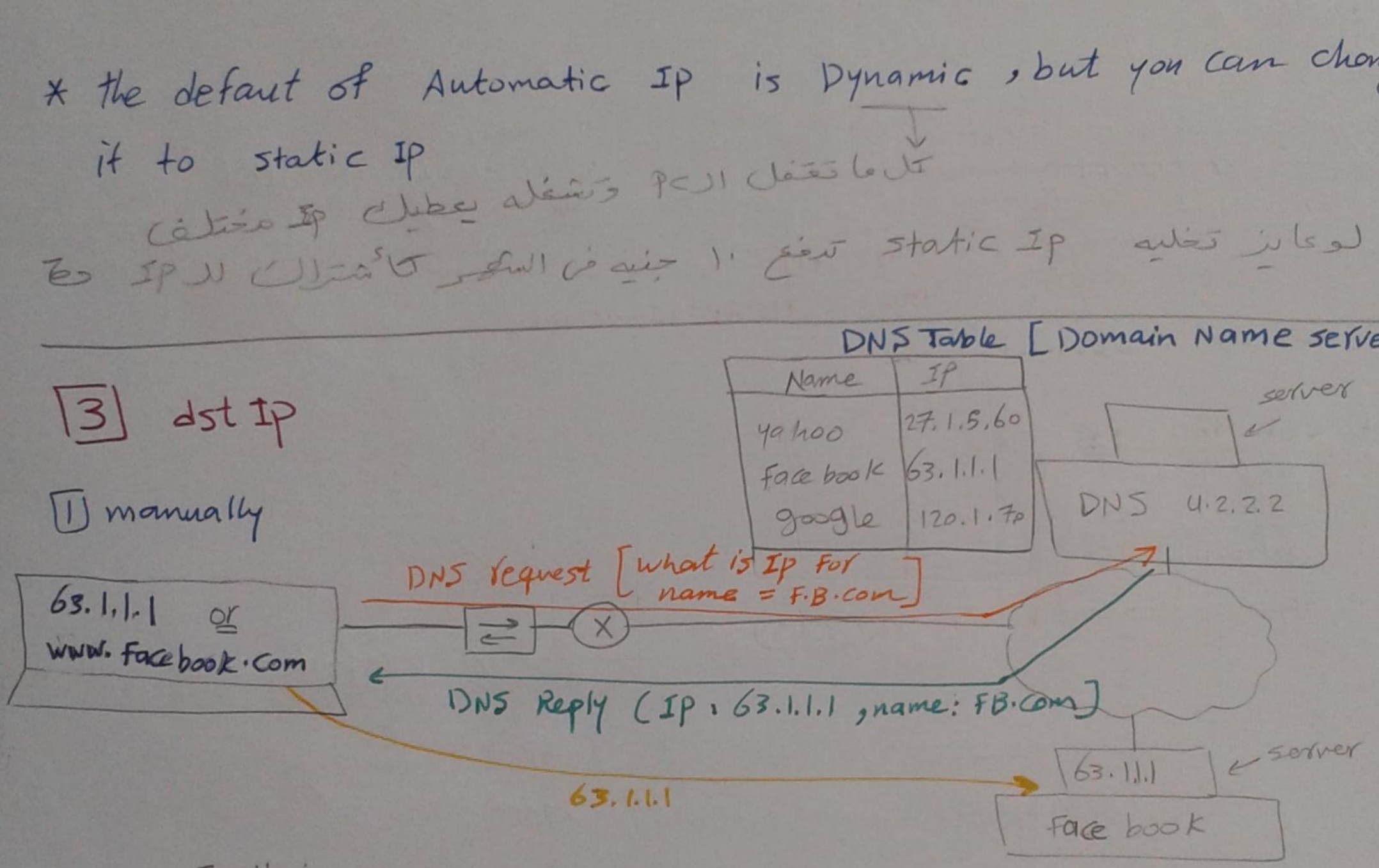
Dynamic ← كل ما تقفل الـ PC وتشغله يعطيك Ip مختلف

لو عايز تخليه static Ip تدفع ١٠ جنيه فى الشهر كاشتراك لل Ip

---

3 dst Ip

1 manually



* الـ DNS عبارة عن Internet book زى الـ phone book اللى عندك فى البيت

* معناه تكتب الـ Ip بتاع الموقع اللى انت عايزه فى URL وهو هيوديك لـ server على طول

* او تكتب اسم الموقع www.facebook.com وهنا انت هتبعت request لـ DNS server وهو هيبعت لك الـ Ip بتاع الـ Facebook

* يوجد 13 DNS server حول العالم [٨ منهم فى امريكا] وياخدوا الرموز من A ← M

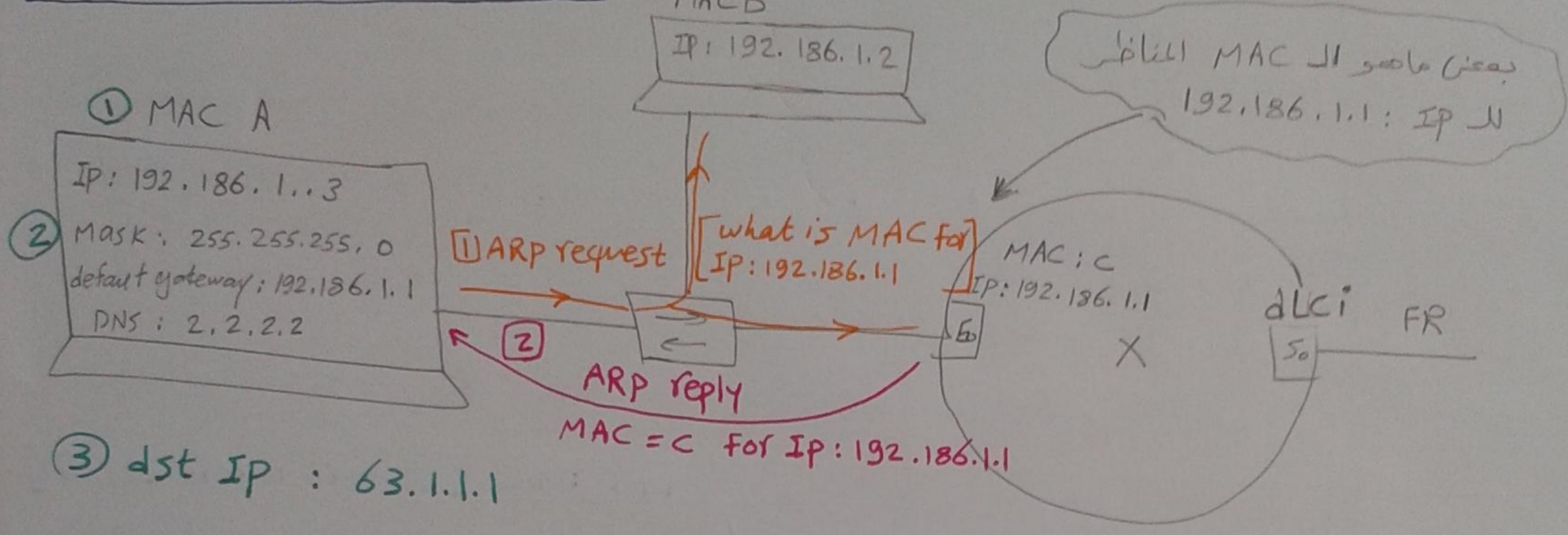
* شركات الـ service provider زى [TE data] بتاخد نسخه من DNS server وتسطبها عندها وانت لما بتعمل request على موقع معين بتروح على الـ server بتاع الـ TE data ويجيبلك الرد ولو الـ server بتاع الـ TE data متعرفش الموقع بقى هيروح على الـ DNS server الاصلى ويعرف منه عليه الـ Ip بتاع الموقع اللى انت عايزه

3 dst MAC [next hop MAC]

ARP : address resolution protocol

next hop MAC اقدر اعطيك dst Ip بمعلوميه ال ⇐ ARP طريقة عمل ال

cas.1 : If dst ip in the same LAN



③ dst Ip : 63.1.1.1

④ dst MAC ?? ⓒ

③ ARP Table

IP	MAC
192.186.1.1	C

* ① ال PC هيبعت ARP request ودة نوعه Broadcast
* ② ال Router اللى يملك ال Ip (192.186.1.1) هو بس اللى هيرد
* ③ ال PC هياخد الرد دة و هيخزنه فى جدول اسمه ARP Table

[اكتب على ال Dos الامر دة ARP -a عشان يطلعلك الجدول بتاع ال ARP]

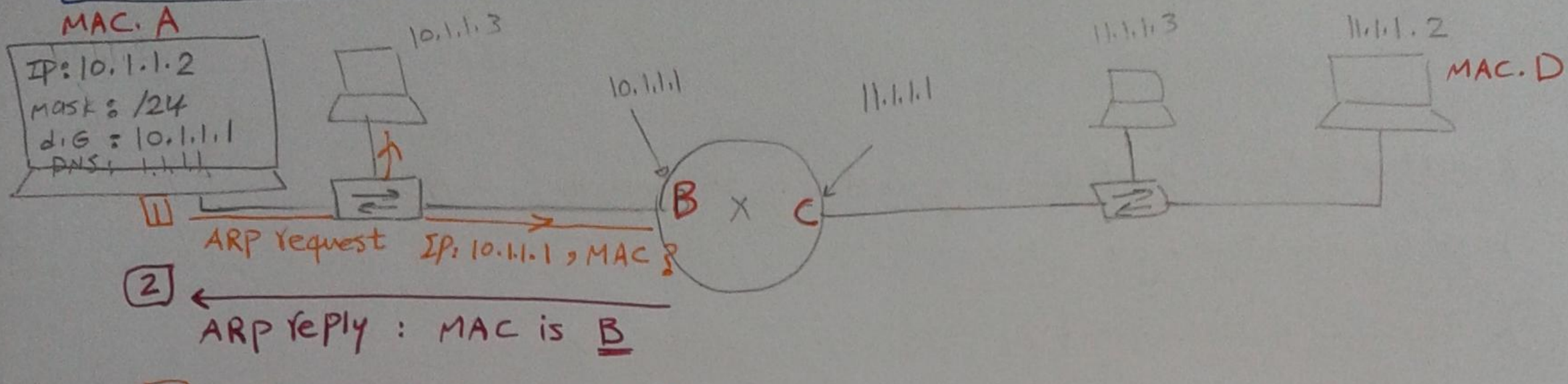
---

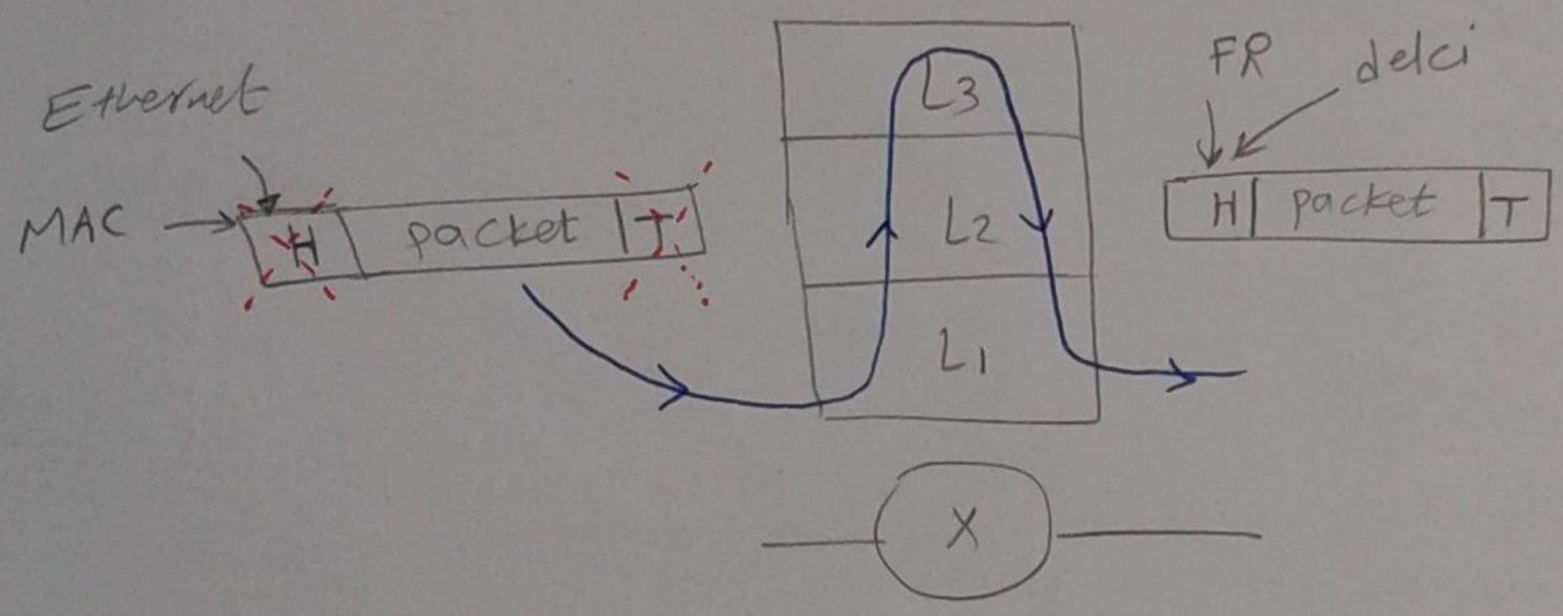
* كل الشرح اللى فوق دة فى حالة ال LAN ، نيجى بقى فى حالة ال WAN

* فى حالة ال WAN هنفترض بقى انه ال Final end Ip موجودة فى LAN تانية

case:2 : If dst Ip in another LAN

sometimes called proxy ARP





* ملاحظة: الـ dst IP & src IP مستحيل يتغيروا لكن الباقي بيتغيروا

dst MAC & src MAC

* ملاحظة: الـ ARP بتتعرف في Layer 2

PDU [packet data unit] = segment

layer 4: Transport layer

it is responsible for end to end delivery control

1- segmentation : by deviding data in to smaller parts

2- error detection : by CRC

3- session addressing : by port no. → ايه هو الـ Application اللي عايز تتكلم معاها؟ في الـ PC اللي انت عايزة

port no 16 bit [0 – 65535]

0 — 1023

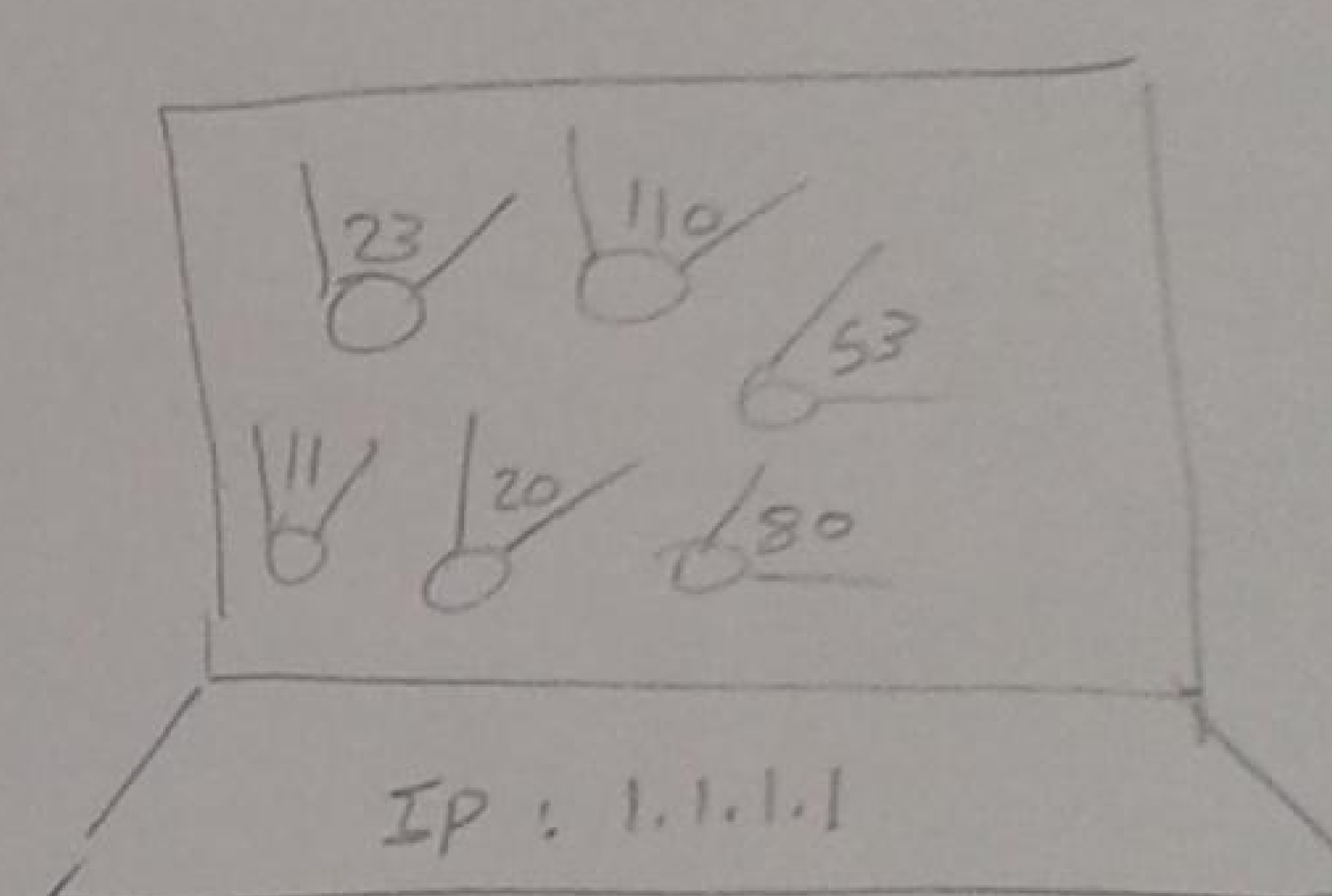
* regestered ports [well known ports]
* used by servers

20, 21 → FTP
23 → Telnet
25 → SMTP
110 → POP3
53 → DNS
80 → HTTP
443 → HTTPS ← security

1024 – 65535

* un regulated ports
* session address for users

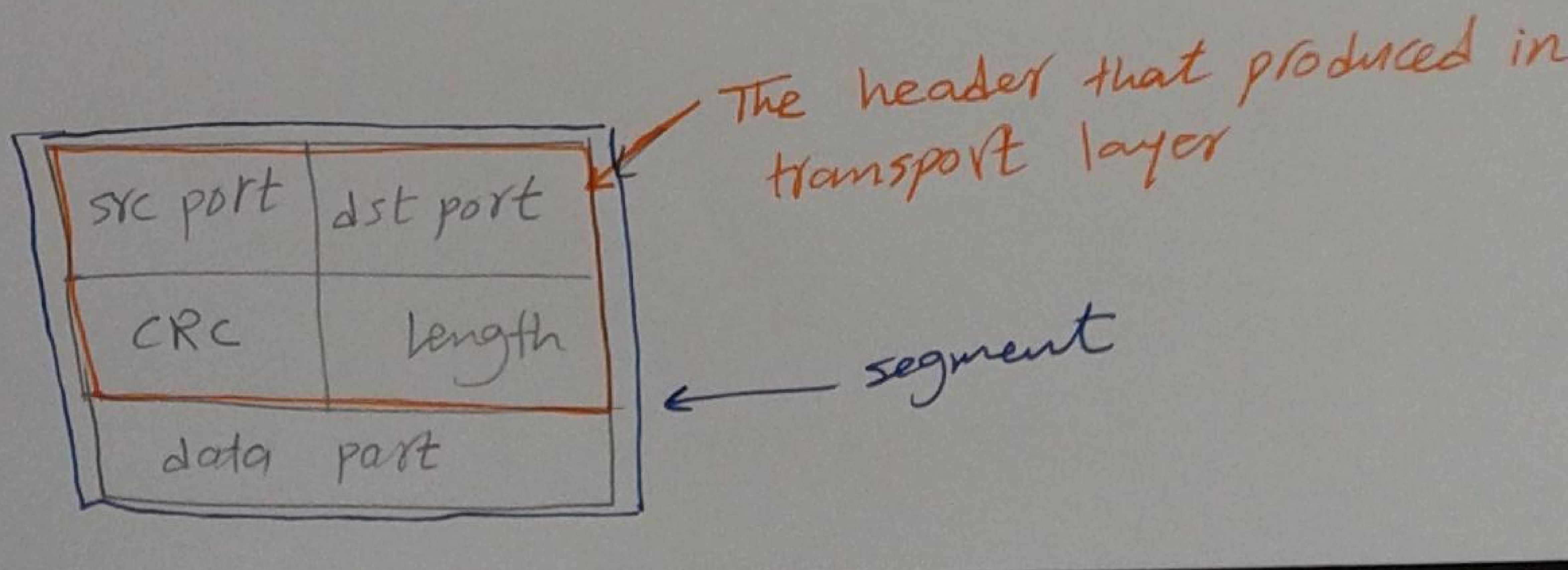
لو انت عايز تخلي server يعمل عمليات معينة

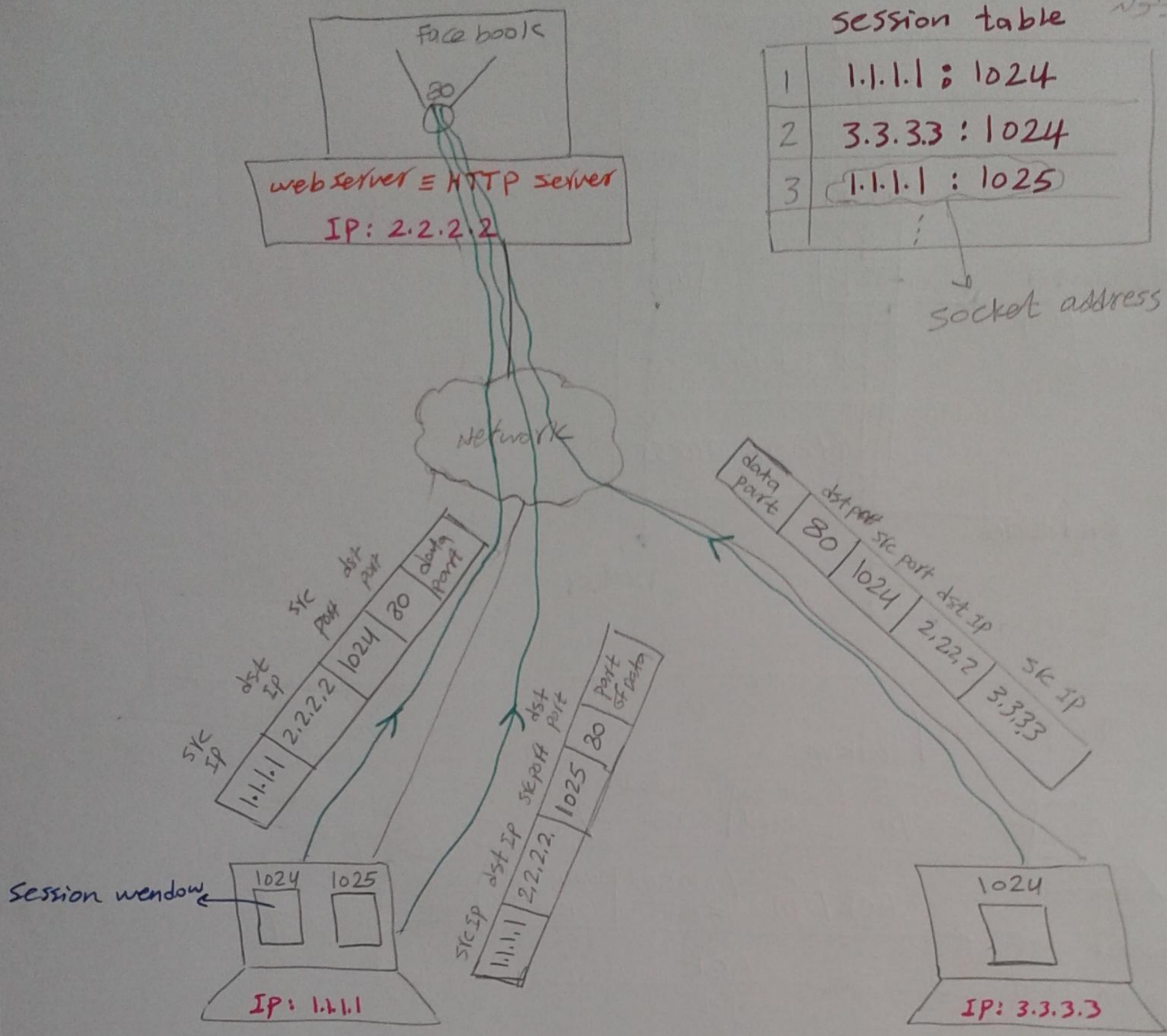


* socket no = 48 bit or [socket address]

IP : port
32 bit : 16 bit

الـ socket address ده بيعتمد على فكرة التخفيس في IP واحد
زي عندك في البيت انه اكتر من PC على نفس الروتر





---

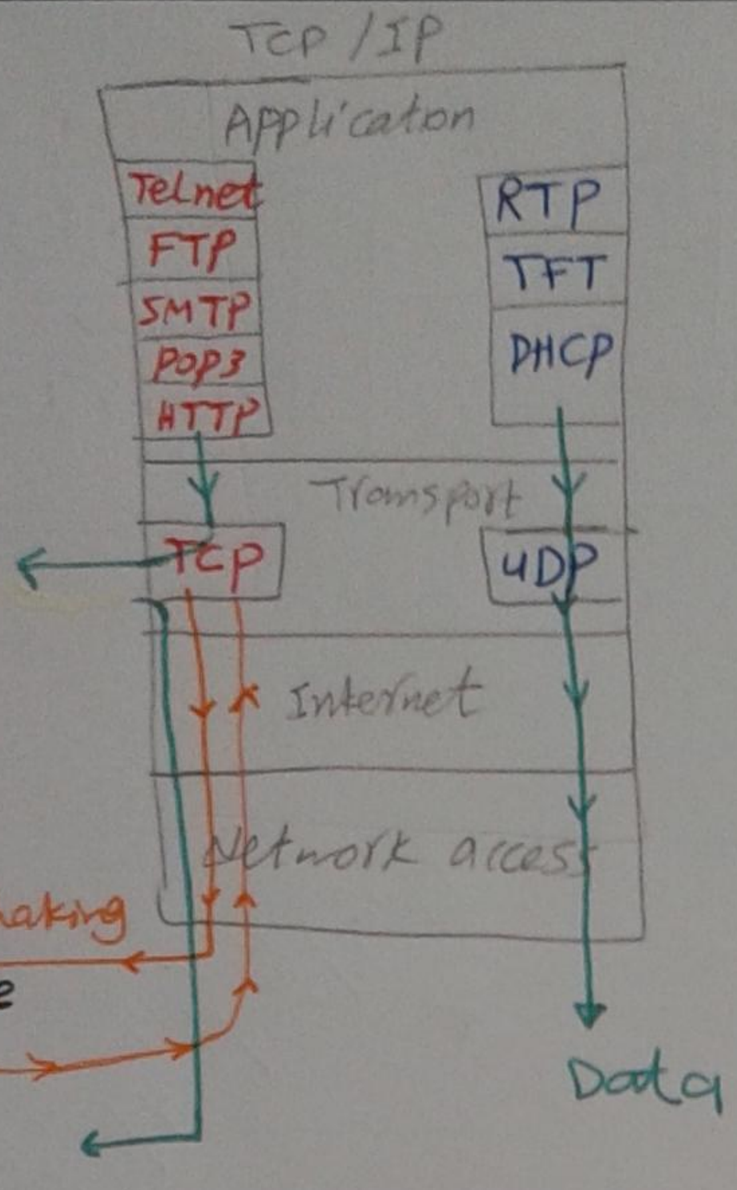
④ Transport layer provide two services

① Connection less service by UDP [User Datagram protocol]

② connection oriented service by TCP [Transmittion control prot]

- the services that interest in speed as [RTP] and [TFTP]
  - RTP: Voice, Vedion
  - TFTP ← Trivial Transfere protocol ← عامل زي FTP بس على احجام صغيرة
- * يعني ان UDP مش شرط يتأكد ان الداتا توصل لل dst ولا لأ
  يعني انه يخرج في الحال

Telnet - FTP - SMTP - POP3 - HTTP زي Applicat اللي محتاجه دقه ← لو حد ك Handshaking Msg يبعت ويبعت عدة
يعني انه لما تيجي داتا يجربها عدة مرات يتأكد هل الداتا بتوصل ولا لأ

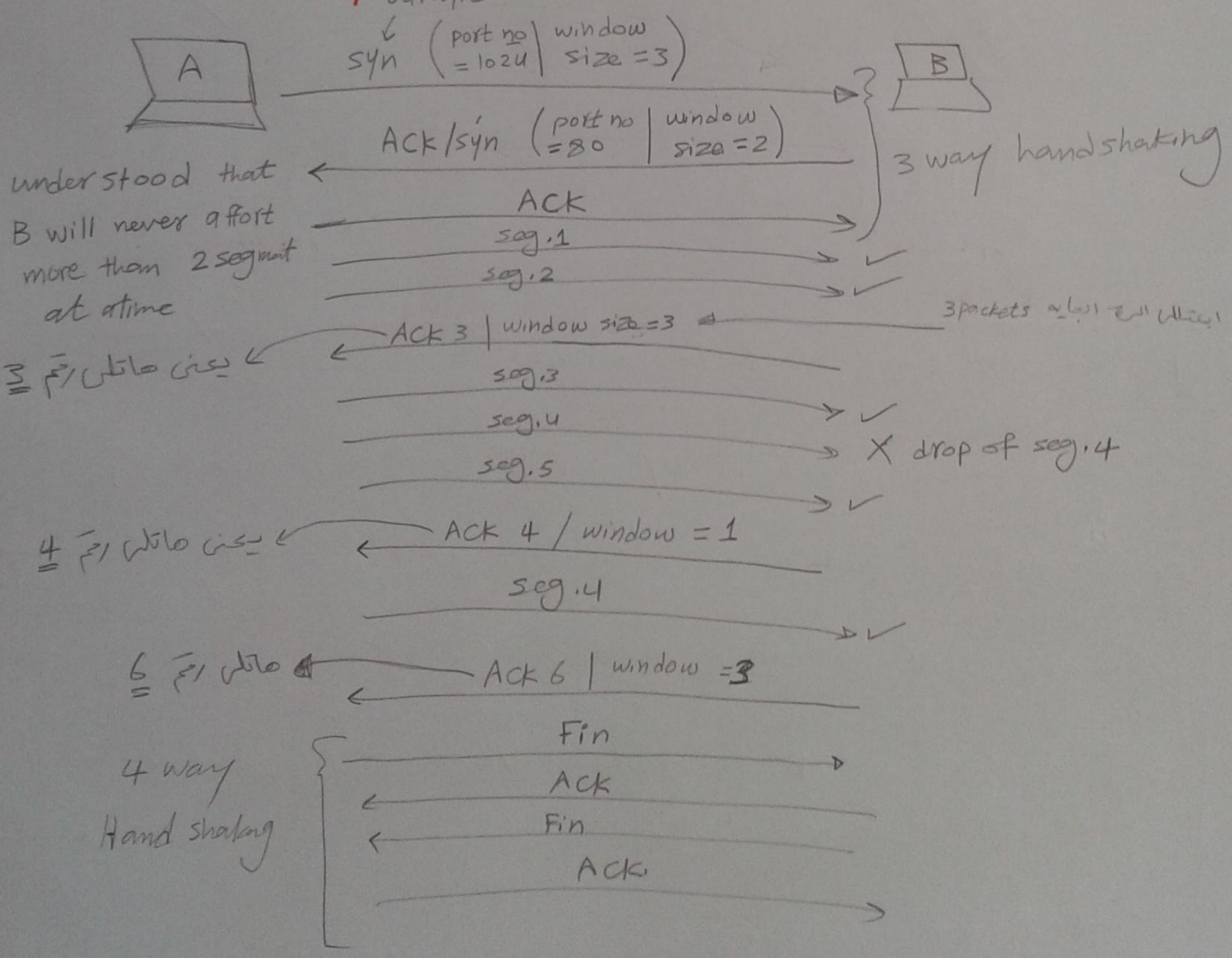


parking of ① data untill hand shaking operation will be success

② Handshaking

---

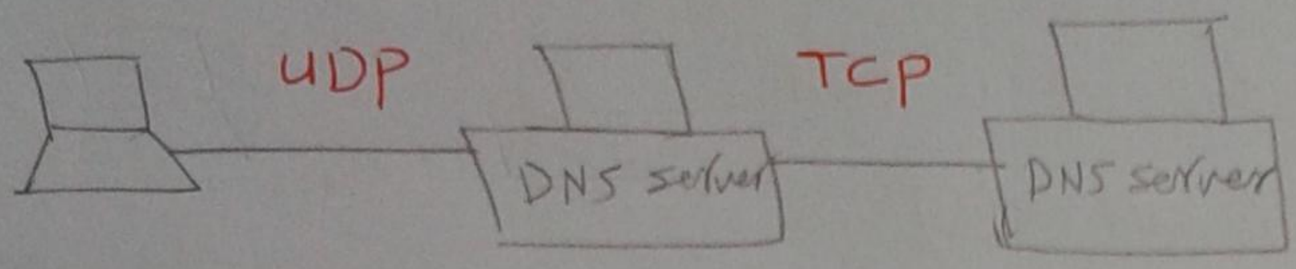
* For TCP only



Interview @uestion

ق : ال DNS بيشتغل مع TCP و UDP

Sol : الاتنين



Note in subnets :-

* old subnetting standard : while subnetting , don't use first and last subnets

→ leave them for future → no of subnets = $2^{SN} - 2$

* new subnetting standard : you can use all subnets

Routing Introduction

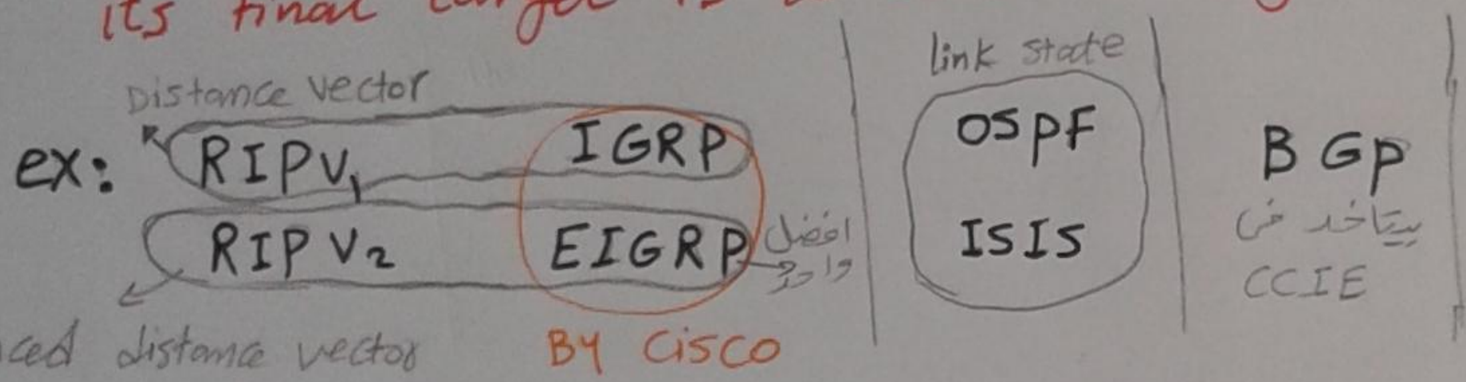
* Routed protocol : it is used to carry user data triffic from end to end
موجّه - متوجّه → مطول به

by - encapsulating data end to end
- supporting logical addressing

ex: IPV4 - IPV6 - IPX - AppleTalk

* Routing protocol : it is the exchange of information between Routers
فاعل → موجِه , so as each Router tell the other about networks it can reach

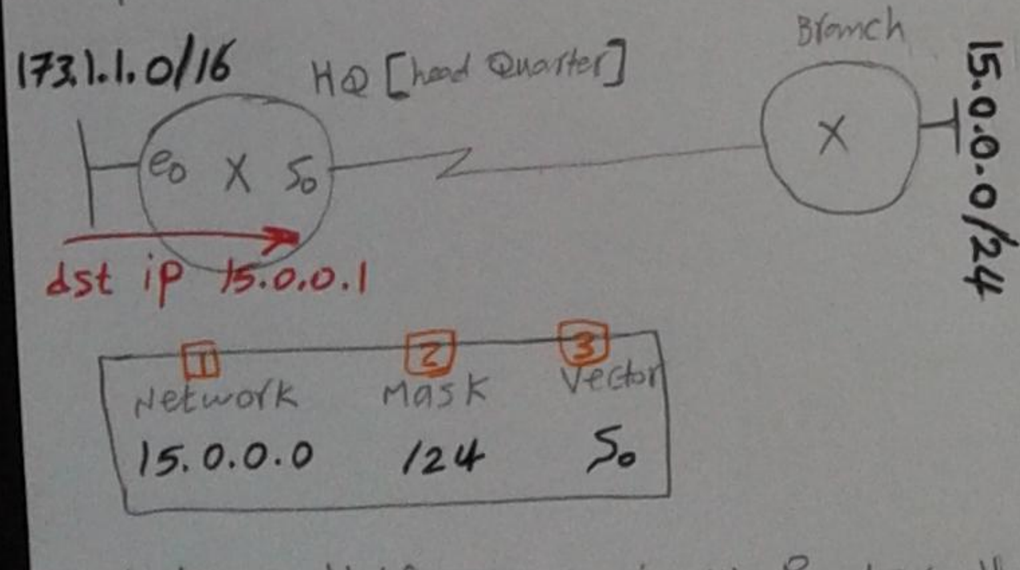
its final target is to build Routing table [Network MAP]



Routing classification

Static Routing

* building the routing table manually
* used for simple Networks
only one path exist to dst Network



static الى فى البيت شغال Router الـ
والـ Routing table معمول غير سطرين

Dynamic Routing

* Building routing table automatically by s/w called routing protocol
* used If Network is complex
more than one path exist to dst

Dynamic Routing

IGP [interior Gateway protocol]

"routing protocols that work inside Autonomous system"

ex
- Distance vector (D.V) [RIPv1 & IGRP]
- advanced D.V [RIPv2 & EIGRP]
- link state [OSPF & ISIS]

EGP [exterior Gateway protocol]

"routing protocols that work between Autonomous systems"

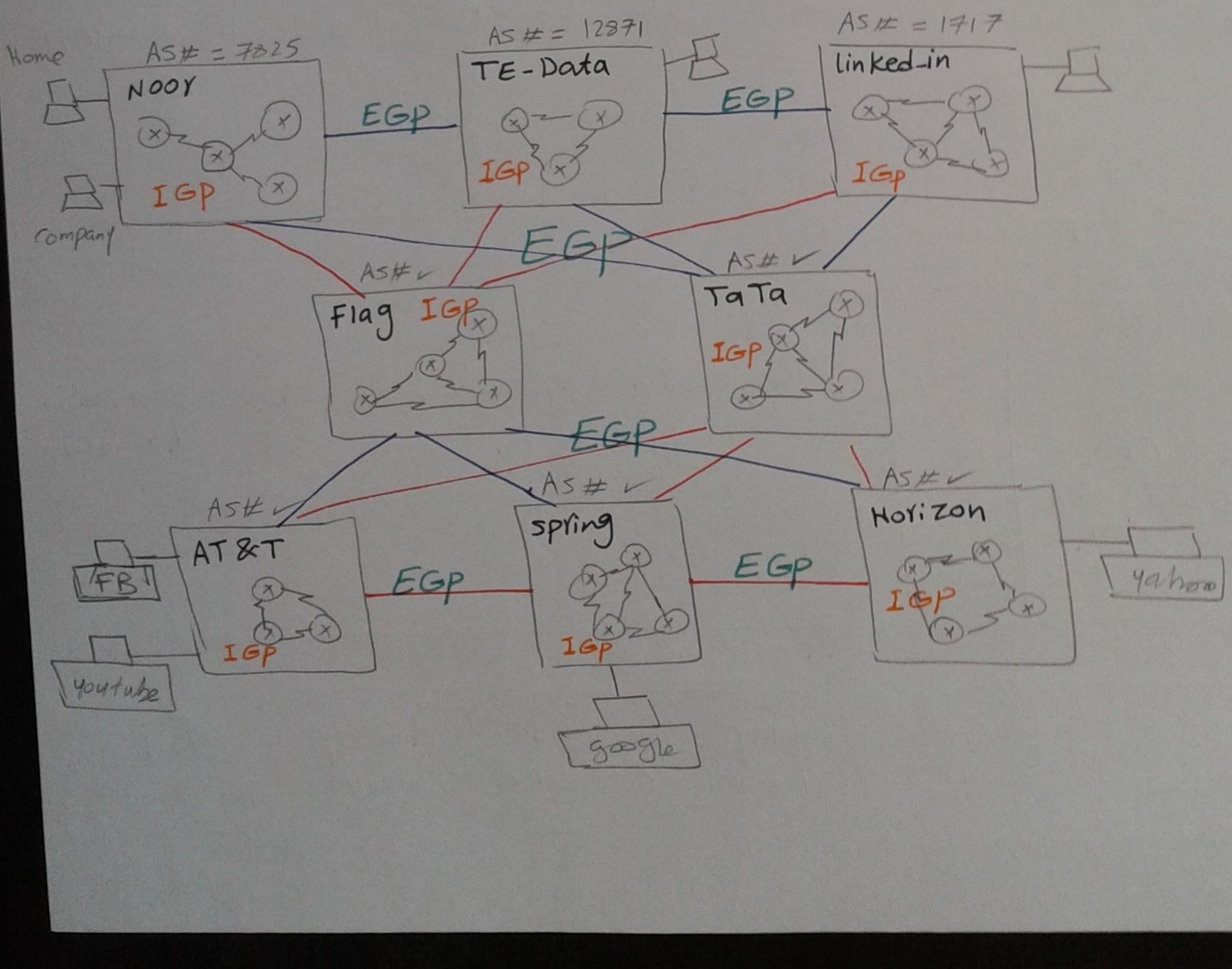
ex: EGP [old]
BGP [New] [Boarded Gateway protocol]

وده شغال كـ Translator بين الـ Autonomous systems (يعني)

Automomous system : نظام مستقل

it is a group of devices that is under single Technical Administration or under single routing policy

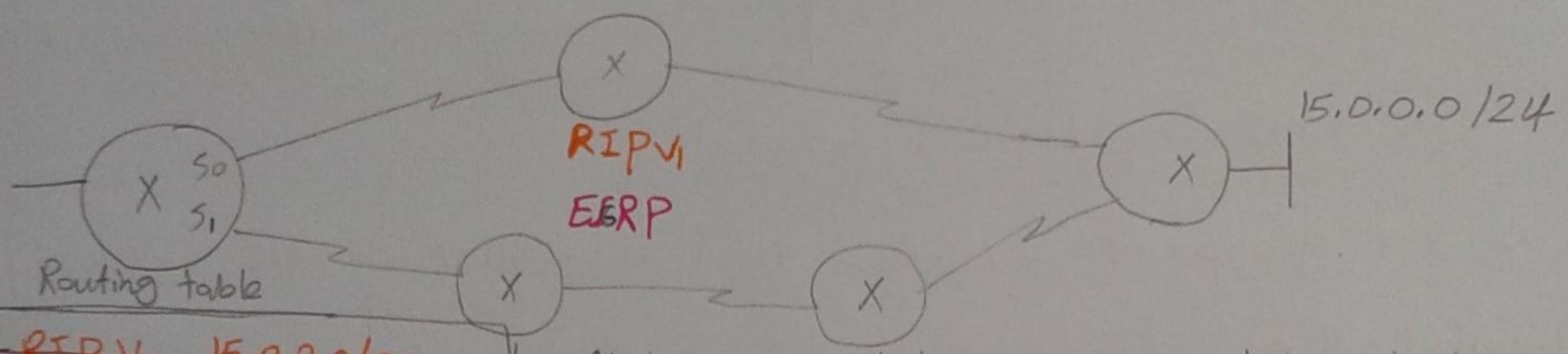
Autonomous sys (AS) number → [0 → 65535]



* Routing table :- it contains :-
  - the best protocol [If many exists]] → it has the best of the best
  - the best path [If many exists]]

* the best protocol is protocol that having least administrative distance

admin. distance / it is a number from [0 - 255], each routing protocol has a unique no, that number reflect thruthFullness [preference] of protocol



→ It is canceled because admin distance is high 120

لو فى طريقين فى نفس الـ protocol يوصلوك لـ Network معينه ⇐ الـ Router هيختار افضل طريقه ودة بيعتمد على الـ Metric (المسافه) [الاقل مسافه هو اللى هيكمل فيه وهيحزف الطريق التانى] ☺

The best path is having the least Metric ≡ cost مسافه

IETF : internet engineering ← اسم الهيئه اللى بتحط الـ admin. distance

protocol	admin. distance
RIPv1, v2	120
ISIS	115
ospf	110
IGPR	100
EIGPR	90
BGP	20
Static	0, 1

The best the protocol, the least the admin. distance

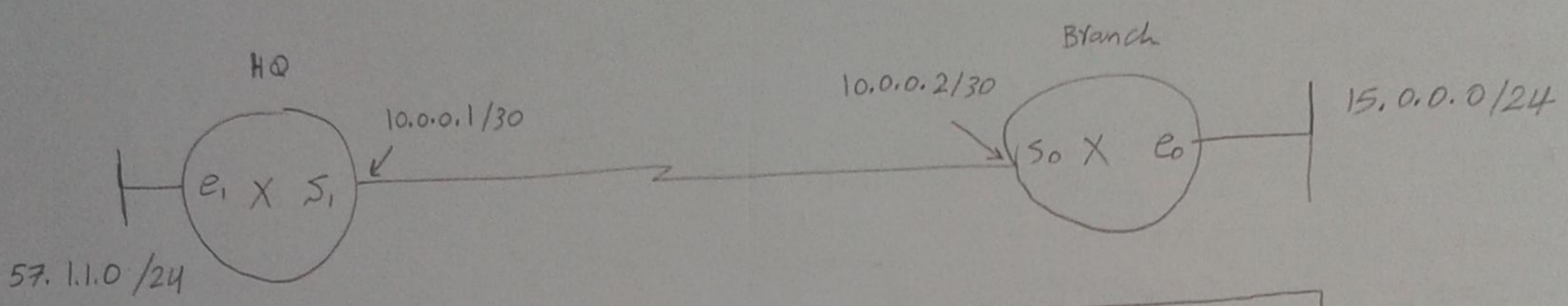
metric ≃ cost

- hop count: no of routers; ex: RIP V1, V2
- Bandwidth (speed): Metric ∝ 1/BW
- delay (late)
- load (congestion) الحمل
- reliability (stability)
- MTU [Maxi. Transfere unit] packet الـ

* Static Routing

[1] Connected Networks ⟶ (C)
[2] Static Route ⟶ (S)
[3] Static to all ⟶ (S*)

← Routing table الروتر فى ال



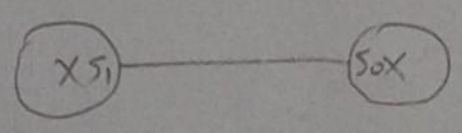
Connected ←
C 57.1.1.0/24 e1
C 10.0.0.1/30 S1
static ← S 15.0.0.0/24 S1

C 15.0.0.0/24 e0
C 10.0.0.2/30 S0
Static to all ← S* 0.0.0.0/0 S0

(Config) # ip route | Network (1) | Mask (2) | { name of exit interface | or - IP of next hop - - - - Router - - - - gateway } (3) Vector

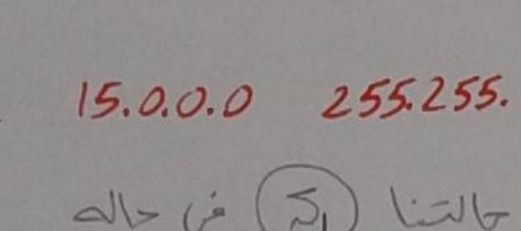
* HQ (Config) # Ip route 15.0.0.0 255.255.255.0 S1 → admin distance = 0

point to point topology فقط S1 انت بتكتب اسم ال interface اللى فى حالتنا



* HQ (Config) # Ip route 15.0.0.0 255.255.255.0 10.0.0.2/30 → admin distance = 1

انت بتكتب اسم ال Vector [10.0.0.2/30] فى حالة لما تكون الشبكة star topology يعنى point to Multipoint



Branch (Config) # ip route 0.0.0.0 (Network 1) 0.0.0.0 (Mask 2) S0 (vector 3)

+ (Config) # IP classless

The First 1.15 hr is Lab

Routing classification

- Dynamic Routing
  - IGP
    - Distance vector
      - RIP V_1
      - IGRP
    - Advanced D.V
      - RIP V_2
      - EIGRP
    - link state
      - OSPF
      - ISIS
  - EGP
    - ex: EGP , BGP
- Static Routing

---

* Distance vector (D.V.)

ex: - RIP V_1 : Routing information protocol V_1

- IGRP : interior Gateway Routing protocol [by cisco]

* D.V. operation

① at start up = just after configuration

② at convergence = steady state

③ at change = If new network appears or network disappears

* في ال D.V protocol ، انا هحسب ال Metric عن طريق عدد ال hops

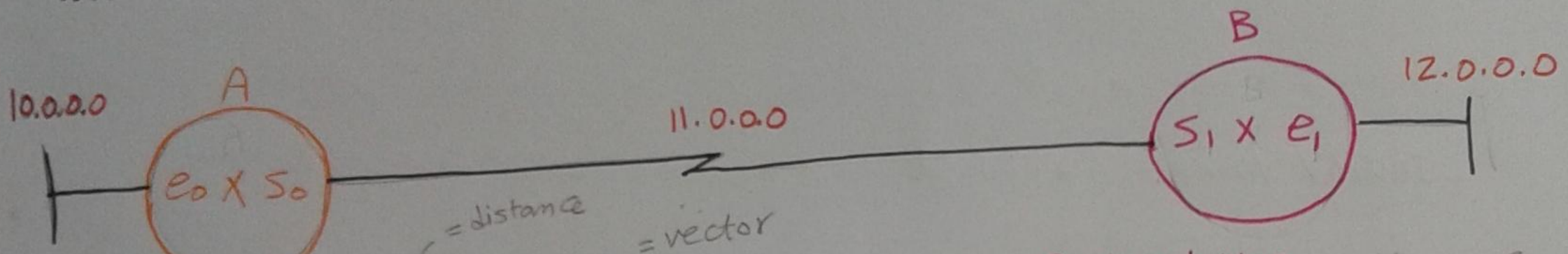
* each 30 sec , each Router will send its Routing table In IP packet whose IP = 255.255.255.255

* this IP is the <u>Direct Broadcast IP</u> that <u>Force</u> (يجبر) all Routers connected to our Router to <u>process</u> the packet that includes the routing table

* note , the Router can send Broadcast Msg . but It doesn't route (يوجه) the incoming Broadcast Message

يعني انه الروتر ينفع يرسل Broadcast لكن لو جاتله Broadcast مش هيوديها وهياخدها لنفسه

[1] at start up :
each Router will take a copy of all Routing table entries, add (1) me to the metric & send the modified entries out of all its interfaces periodically



Routing table·A

			metric	interface
C	10.0.0.0		0	e_0
C	11.0.0.0		0	S_0

Connected

Routing table·B

		metric	interface
C	12.0.0.0	0	e_1
C	11.0.0.0	0	S_1

* After 1st periodic update (30 sec)

Routing update [Routing advertisement] ← Text

11.0.0.0 , (1) → you can reach this Network by one hop
10.0.0.0 , (1) → who is me
as above

12.0.0.0 , 1
11.0.0.0 , 1

admin. distance ⟹ represent how Metric is.

ملحوظه / كل Router هيعمل الـ update بعد 30 ثانيه من ساعته الخاصه يعني مش شرط الاثنين يعملوا update في نفس اللحظه

C	10.0.0.0	0	e_0	
C	11.0.0.0	0	S_0	← 0
~~R~~	~~11.0.0.0~~	~~1~~	~~S_0~~	← 120
R	12.0.0.0	1	S_0	

RIP

هنا الروتر وجد عنده الـ Network 11.0.0.0 متسجله عنده مرتين ← هيشوف الـ admin distance بتاع كل سطر وهيحزف السطر اللي فيه الـ admin distance عالي

C	12.0.0.0	0	e_1
C	11.0.0.0	0	S_1
~~R~~	~~11.0.0.0~~	~~1~~	~~S_1~~
R	10.0.0.0	1	S_1

* After 2nd periodic update

10.0.0.0 , 1
11.0.0.0 , 1
12.0.0.0 , 2

12.0.0.0 , 1
11.0.0.0 , 1
10.0.0.0 , 2

C	10.0.0.0	0	e_0	
C	11.0.0.0	0	S_0	
R	12.0.0.0	1	S_0	
R	12.0.0.0	1	S_0	← still alive
~~R~~	~~11.0.0.0~~	~~1~~	~~S_0~~	
~~R~~	~~10.0.0.0~~	~~2~~	~~S_0~~	

لو الـ Router وجد انه في سطرين ليهم نفس الـ Network ونفس الـ admin distance ⟸ هيحزف اللي still alive دي الـ Network انه الـ Router موجودش عن الشبكه

C	12.0.0.0	0	e_1	
C	11.0.0.0	0	S_1	
R	10.0.0.0	1	S_1	
R	10.0.0.0	1	S_1	← still alive
~~R~~	~~11.0.0.0~~	~~1~~	~~S_1~~	
~~R~~	~~12.0.0.0~~	~~2~~	~~S_1~~	

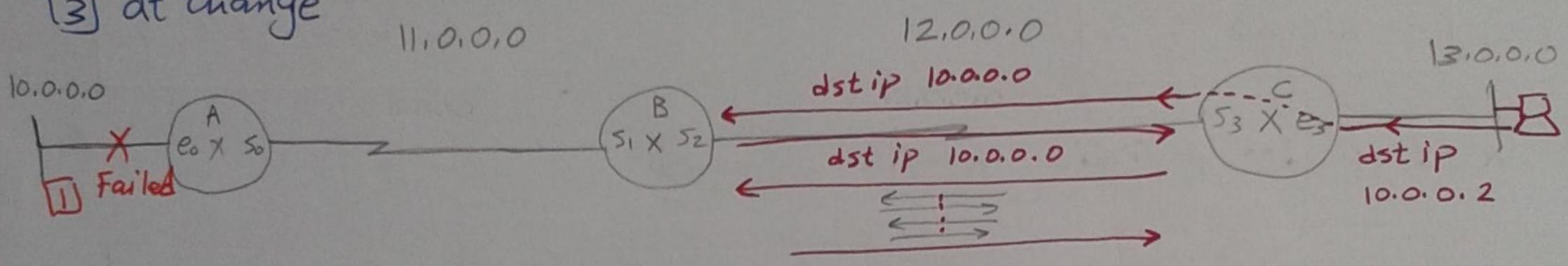
[2] at convergence [steady state]
although convergance, there is still periodic upade to be sure that Networks are still alive

* عشان يعرف الشبكه وقعت ولا لأ ضيعمل invalide timer ⟵ يعني لو شبكه وقعت
الروتر هياخد القرار انه يحذفها من الجدول بتاعه لكن قبل ما ياخد القرار ده
هيقول اصبر عليها يمكن هي مازالت موجوده لكن في مشكله بسيطه وهتتحل

Invalid timer = 6 * updates = 6 * 30 sec = 180 sec = 3 min.

---

[3] at change



[2] After 30sec ←

metric vector

~~C~~	~~10.0.0.0~~	~~0~~	~~e_0~~
C	11.0.0.0	0	s_0
R	12.0.0.0	1	s_0
R	13.0.0.0	2	s_0

[3] after 30 sec →
10.0.0.0 , 16 = ∞ [unreachable]
11.0.0.0 , 1
12.0.0.0 , 2
13.0.0.0 , 3

C	11.0.0.0	0	s_1
C	12.0.0.0	0	s_2
[4] R	~~10.0.0.0~~	~~1~~	~~s_1~~
R	13.0.0.0	1	s_2
[4] R	10.0.0.0	3	s_2

[5] after 2nd 30 sec →
11.0.0.0 , 1
12.0.0.0 , 1
13.0.0.0 , 1
10.0.0.0 , 16

C	12.0.0.0	0	s_3
C	13.0.0.0	0	e_3
R	11.0.0.0	1	s_3
R	10.0.0.0	2	s_3

[4] ←
13.0.0.0 , 1
12.0.0.0 , 1
11.0.0.0 , 2
10.0.0.0 , 3

⟵ هيضيف السطر ده في Routing table بتاع Router B

there are two problems :-

[1] slow convergence

في حاله ان 10.0.0.0 وقعت * اولا RouterA هيعرف الاول . ثانيا من RouterB
هيعرف ان 10.0.0.0 وقعت الا بعد 30 sec عن طريق RouterA وكمان RouterC
من هيعرف الا بعد 30 sec عن طريق RouterB ← يعني RouterC عرف بعد 60 sec

[2] L3 Routing loops → التوضيح في الرسمه فوق

[1] الشبكه 10.0.0.0 وقعت
[2] RouterA هيحذفها من الجدول بتاعه وهيبعت [3] لـ RouterB بعد 30 sec *معلومه تفيد
ذلك بالاضافه 10.0.0.0 , 16 وهنا معنى ∞ = 16 . والرقم 16 تم حسابه
على اساس ان اقوى Autonomus system في الوقت ده لا تزيد عدد الـ Hops
فيه عن 16 hop [لا يمكن ان يتم 16 hop او بعض في نفس AS وعشان كده الـ RIP
بيستخدم في الشبكات الصغيرة]

4 Router B هيحذف الـ Network 10.0.0.0 من عنده

5 بعد 30 sec Router B هيبعت update لـ Router C بأن 10.0.0.0 مش موجودة بنفس الامر اللي فات

← لكن هنلاقي المشكلة في خطوة 4 وهي حالة انه قبل الـ 30 sec بتاع الـ update بتاع Router B هو وصل Router C وارسله الى Router B . في الحالة دي Router C هيرسل 10.0.0.0 و 3

* صنابقي الازمه في انه Router B هيقارن المعلومه اللي وصلتله من Router A [10.0.0.0 و 16] والمعلومه اللي لسه واصله من Router C [10.0.0.0 و 3] وهيضطر انه يحذف سطر من الاتنين ← فهيحذف الطريق الاسوأ [10.0.0.0 و 16]

* صنابقي لو جه PC ذات IP = [13.0.0.2] وعايز يكلم حد من Network 10.0.0.0 ⇐ Router C هيقول لـ packet انه الطريقه لازم تروح له ناحيه Router B عشانه هو جايب اسم الـ Network 10.0.0.0 منه و لما تروح الـ packet لـ Router B هيقولها اذهبي الى Router C عشانه انا اعرف الـ Network 10.0.0.0 من طريقه

و هتفضل الـ packet تلف حولين الروترين B&C

⇐ المشكله الاساسيه هنا ان العمليه دي هتشغل الروترات جامد

وكمان الحل في ↓

1 TTL [Time to live] expired

بيساوي الـ TTL دة [256 مرة] كل ما الـ packet تعمل Hop ينقص من الـ TTL واحد لحد ما يبقى خانه الـ TTL في الـ packet = 1 و اول ما الروتر يشوفها بـ 1 هيحذف منه 1 و هيعمل لـ packet ⇐ drop

لكن مازال هتشغل الروترات 256 مرة [كتيييير]

[2] Triggered update + poisoned Route + poison reverse

حل مشكله الـ slow convergence بنسبه ٪100
~ ~ ~ Routing loop بنسبه ٪95

[1] اول ما 10.0.0.0 تقع ← [5] Router A هيتس بيه ويمسحه من الجدول بتاعه Routing table الـ [Immediatly] [3] Router A هيبعت فى الحال لـ Router B وهش هيستنى الـ 30 sec بتاع الـ Routing update
[4] Router B هيمسحه من الـ Routing table بتاعه
[5] Router B هيبعت رسالتين • الاولى (Ack) لـ Router A عشان يقوله الـ update وصل و التانيه هيبعت فى الحال [Imm.] الـ Routng table بتاعه لـ RouterC

لكن المشكله زى المره الاولى لو تم خطوة [4] و Router C بعت الـ Routing table بتاعه قبل Router B بنص ثانيه

⇦ كده احنا وقعنا فى نفس المشكله بس قللنا شبه الـ error (او)

الرسمه اهى

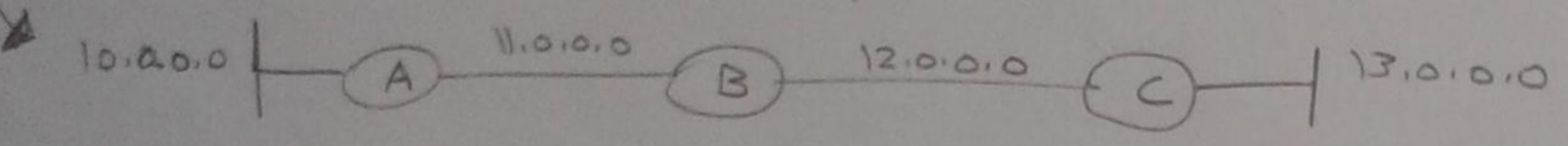
(3) split horizon (الأفق البعيد) : route that learnt from an interface should never be advertized back on the same interface

الراجه اللى ال Router اتعلمها من Interface معين ، مينفعش يعلّمها لـ Router تانى على نفس الـ Interface

[اللى علمنى حاجه ، مينفعش اعلمها له تانى]

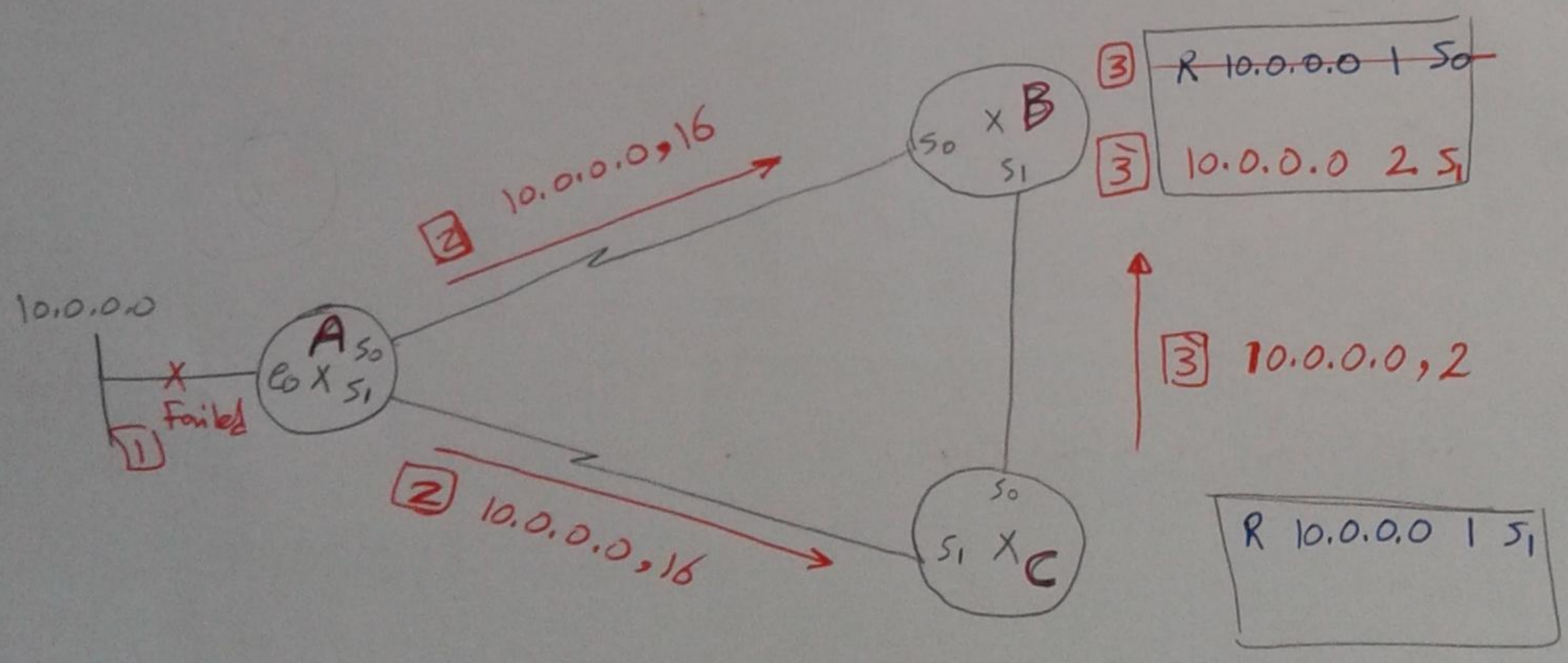
← بمعنى ان Router C اتعلم او اتعرف على 10.0.0.0 عن طريق Router B وعشان كده Router C مينفعش يقول لـ Router B اى معلومه عن الـ Network 10.0.0.0

وتأكيدا انا حليت مشكله الـ loop فى الرسمه اللى فاتت



ولكنه تبقى المشكله فى حاله ان Router C يعرف طريقه تانى يوصل من خلاله لـ 10.0.0.0

← هنا بقى Router C يقدر يقول لـ Router B على السكه التانيه ويحصل Routing Loop تانى كما ترى فى الشكل اوضح



وكانه احل التنين فى الطريقه الجايه [طريقه الصبى]

4 Hold down timer (طريقة الصبر)

← حلت مشكله ال loop 100٪ بس على حساب ال convergence

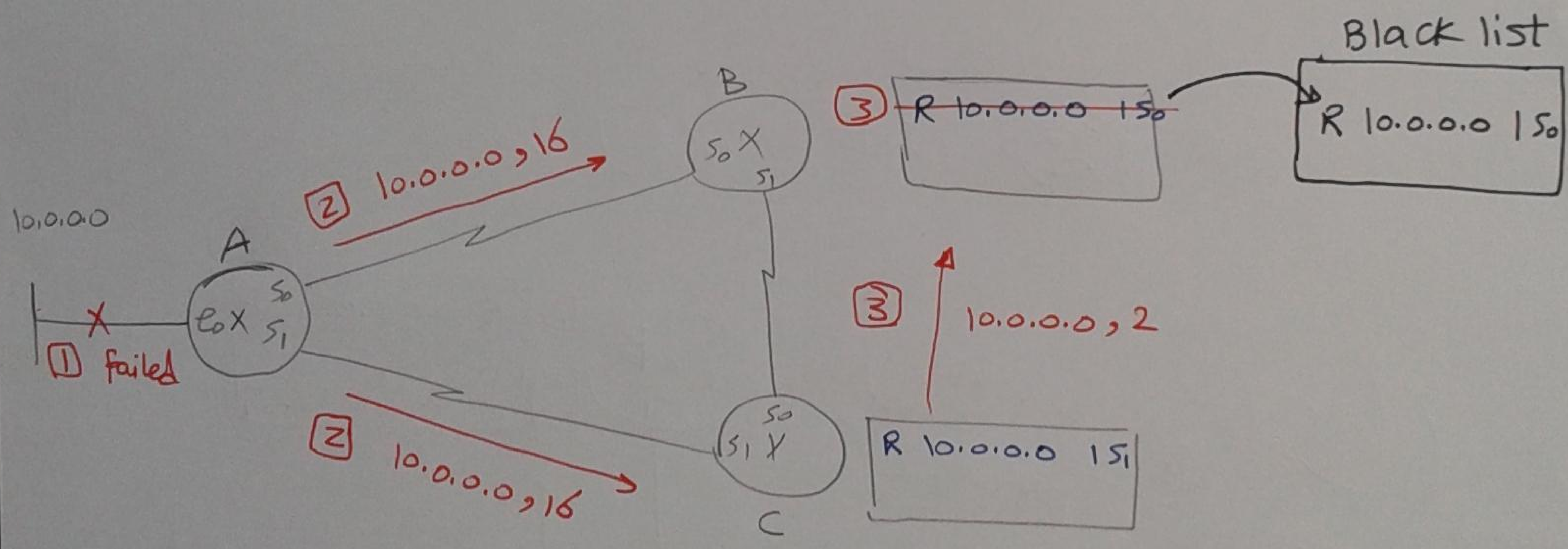
If route failed, donot accept any update about that loop

unless → ① it returns back back [يعني لو جت بنفس الاتجاه و المسافة]

→ ② Hold down time expires [180 sec]

يعني / لو مر 180 sec و الروتر الاخر مازال مصمم انه ال Network موجودة
الروتر بتاعنا هيضطر يصدقه و يعمل update

الحاجه الزيادة هنا انه Router B هيعمل table جديد اسمه Black list
وهيضع في ال Black list الشبكة اللى وقعت (10.0.0.0) ولو اتى له اى upadate
بالشبكه (10.0.0.0) هيلاقيها عندة في الـ Black list ⟸ ومش هينفذ
الـ update الا في الحالتين اللى فوق (مشروحه)



Note: RIP V1 is a class full protocol → doesn't send MASK in updates

RIPv1 C/C's

1- it is Distance vector D.V Standard routing protocol

2- send periodic update every 30 sec out of all interfaces on Broadcast address 255.255.255.255

3- use A- Triggered update + poisoned route + poisoned reverse
B- split Horizon
C- Hold down time (180sec)

4- symbole in Routing table "R"

5- admin. distance = 120

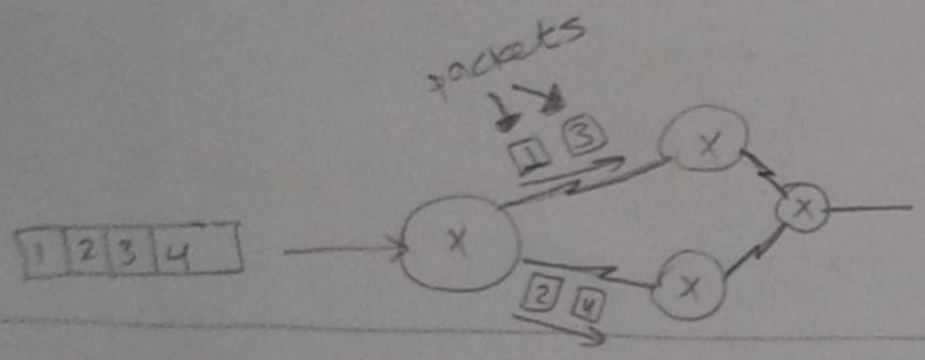
6- metric = hop [max = 15 hop & 16 = ∞]

7- use Bellman ford Algorithm to calculate the best path

8- support Equal load sharing [load balancing] → defaut 4 paths
max → up to 16 or more

9- Class full protocol [doesn't send MASK in update]
The Router that receives the update will estimate the Mask

يستنتج
يعني امر للـ Router كشاب تشتغل بـ 16 طريقة



IGRP C/C's

ملكية
1- it is D.V. Cisco proprietary Routing protocol

2- send -- -- 90 sec -- . 255.255.255.255
↳ is more better because it يوفر the processor & memory

3- use A — — —
B ———
C ——— . (280sec)

4- "I"

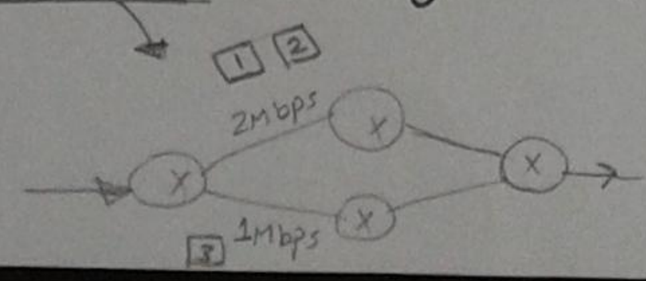
5- 100

6- Metric is composite { B.W , delay , load , reliability , MTU } (default)

7- ———

8- support Equal & unEqual loading sharing [4 default, 60 or more] (امر بتبع)

9- Classfull
يعني لو في طريقين لهم نفس delay & B.W ال

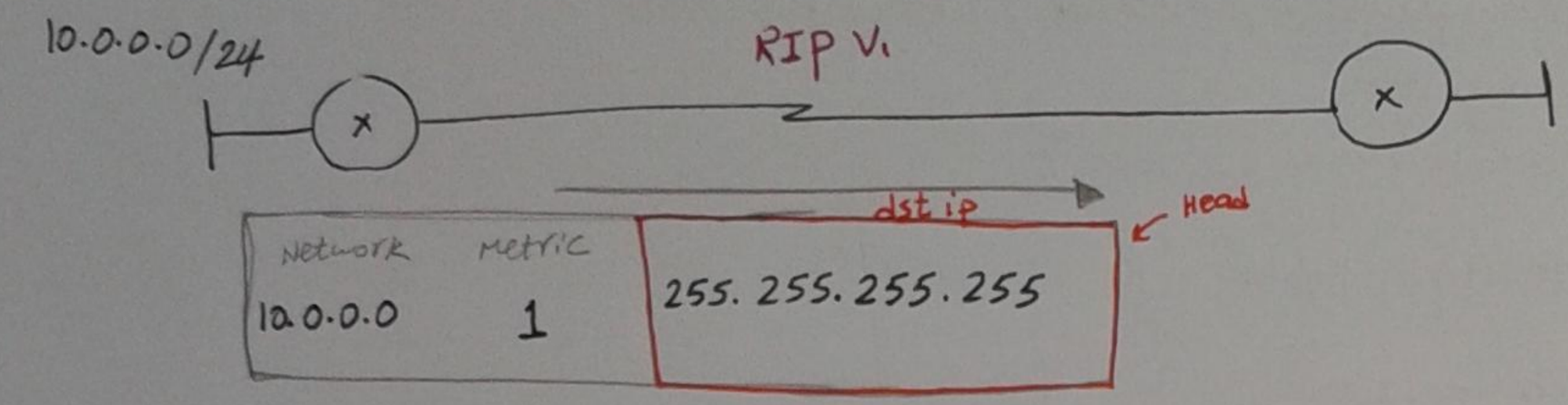


الروتر بيحسب الـ ratio في الـ B.W بين الطريقين ← في حالتنا
2 packet ← 2
1 packet ← 1

Session 13 → 146 minute

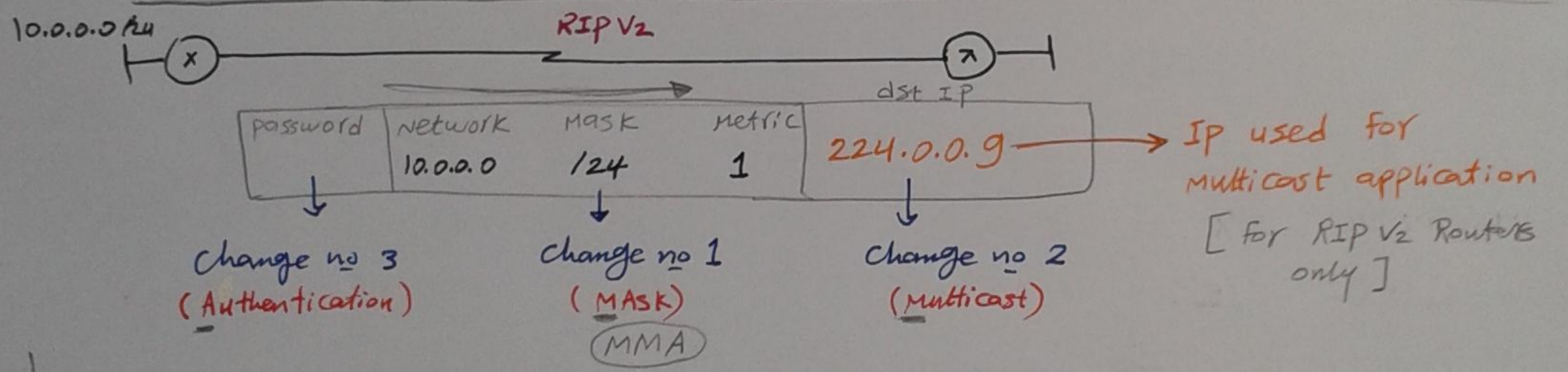
ADVanced Distance vector :- ex: ① - RIP v2 ② - EIGRP

① RIP_{v2} = RIP_{v1} + 3 updates change



المشاكل

1. في RIP V1 كانه الـ Network بيتبعت Classfull بمعنى (doesn't send Mask in updates)
2. الـ Routers بترسل الـ RTG table updates في الـ packet عن طريق العنوان ده 255.255.255.255 (Broadcast) ← المشكلة هنا انه لما تبعت حاجه Broadcast في الـ Network ، انت بتجبر كل الاجهزة في الـ Network انها تعمل process للـ packet دي وبالتالي كل الاجهزة هتشتغل على الفاضي حتى الـ PCs



① التغيير الاول / بعمل الـ Network من Classfull الى Classless وارسل الـ Mask معاه

② التغيير الثاني / حوّل الـ dst ip من Broadcast الى Multicast وبالتالي لما اي Router يبعت update على العنوان ده 224.0.0.9 ← مفيش اي جهاز صيغ الـ update الا لما يكونه العنوان متعرف عنده ، وعشانه اجعل Router يفهم العنوان ده لازم اسطب له S/W خاص للروتر واقوله فيه انت شغال RIP V2

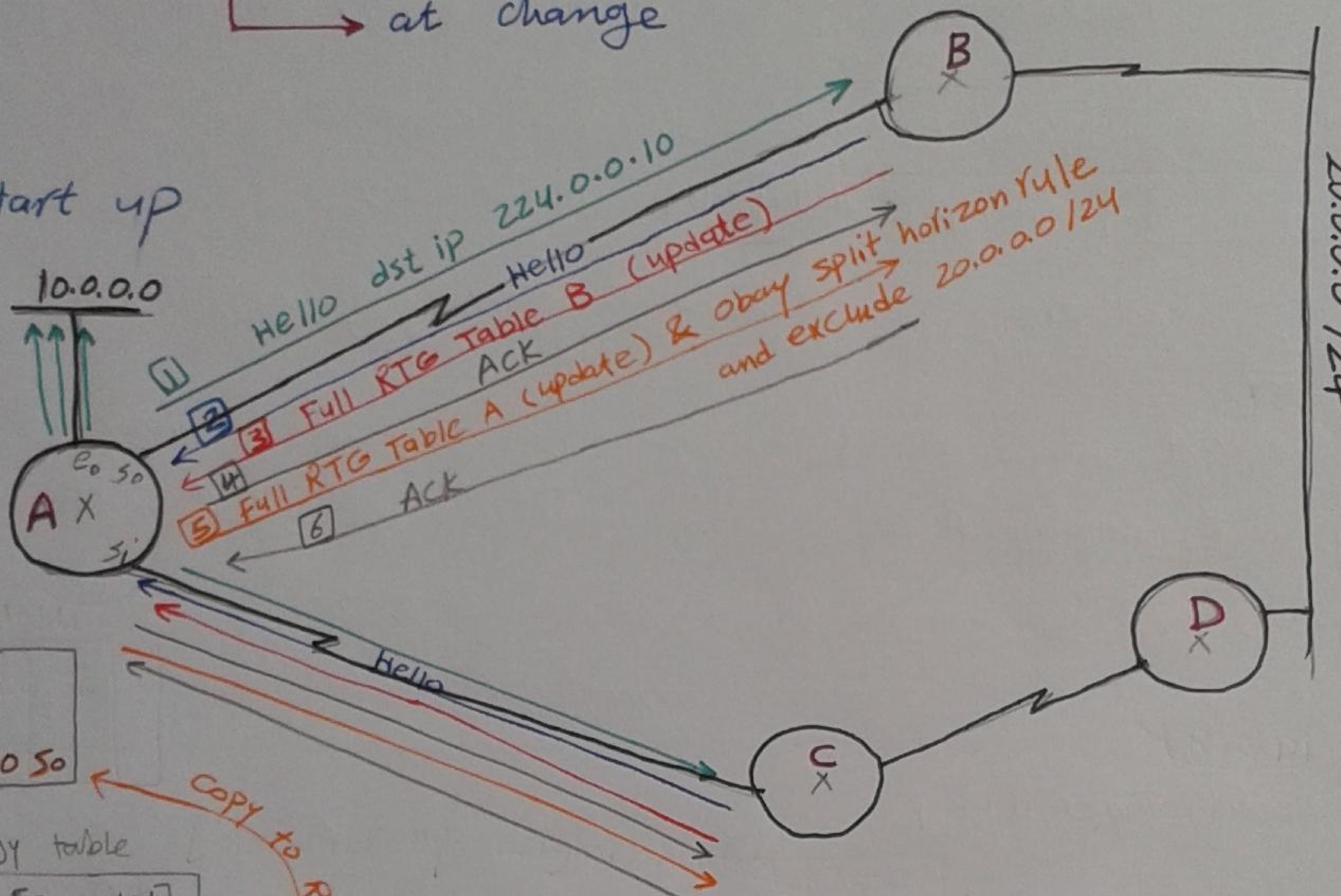
ملحوظه / انا ممكن يكونه عندي Routers شغاله RIP V2 و Routers تانيه مش شغاله RIP V2 ← ملحوظه / لو Router شغال RIP V2 وجاله update على عنوان تاني ما مش صيغوه وميرميه

③ التغيير الثالث / Athentication password وده بحط في كل الـ Routers نفس الـ password وبالتالي لو Router غريب دخل الشبكه وعمل updates وهمية لبقيه الروترات بتاعتي ← الروترات هتعمل check للـ Autho. password ومش هتعمل الـ update

2 EIGRP [Enhanced IGRP]

* EIGRp is type of Advanced D.V
* Its operation
  - → at start up
  - → at convergence
  - → at change

1 at Start up



neighboor table

IP of Neighboor	Interface
Ip of B	S0
Ip of C	S1

Routing table

C ———
C ———
D 20.0.0.0/24 30 S0

Topology table

RTG A [connected devices]
RTGB
D 20.0.0.0/24,30 S0 → S
RTG C
20.0.0.0/24, 70 S1 → FS

Copy to RTG Table

نفس الـ 3 tables اللى موجودين عند RouterA موجودين على Router B & C & D طالما شغالين بنفس الـ protocol

* هنفترض ان Router A لسه جديد فى ال Network وعايز يكوّن Routing table

← اول خطوة هيعملها Router A انه هيبعت Hello Msg على dst ip 224.0.0.10
هنلاحظ ان ال Ip ده نوعه Class D يعنى Multicast IP وبالتالى مش هيفهم ال Ip ده الا الروترات اللى شغاله EIGRP بس

* ميزة ال Hello Msg ان اللى هيرد على Router A ب Hello ، Router A هيرسله الـ upade واللى مش هيرد ، Router A مش هيرسل اليه ال update اصلاً وبالتالى هيريّح الروترات اللى مش شغاله EIGRp والـ PCs من انها تستقبل الـ upade وترميها [يعنى مش هيخليها تستقبل اصلاً]

* الهدف من عمليه ارسال Hello Msg هو ان ال RouterA يعمل Neighbor discovery
والمقصود بـ Neighbor هنا ⇐ ال Routers اللى
Direct connected
under stand same protocol

* ال Direct connected Routers فى حالتنا هما Router B & C
* وهنا بقى هيقوم Router A بعمل ال Neighbor table
ودة جدول للروترات اللى ردت عليه بـ Hello [Exchange of Hello]

IP of neighbor	interface
IP of B	S_0
IP of C	S_1

ملحوظة/ الNetwork 10.0.0.0/24 متسجله عند RouterA ⇐ Static

الخطوة التاليه / إن كلاً من Router B&C هيرسلوا ال Routing Tables بتاعتهم كله الى Router A ، Router A هياخد ال Router tables بتاع C & B ويضعهم فى جدول عنده اسمه Topology table

- ال Topology Table ده بقى عبارة عن Table فى ال Routing tables بتاع Router A & Router B & Router C ، وداخل ال Topology Table ← Router A هيعمل عمليه حسابية اسمها DUAL [Diffusion update Algorithm]

العمليه الحسابيه دى بيتم تنفيذها فى الحاله الاتيه / مثلا Network زى 20.0.0.0/24 ، Router B & Router C حكوا عنها لـ Router A لكن بـ Metric مختلف

فى المثال بتاعنا RTG B كاتب السطر دة

Metric =30	20.0.0.0/24 , 30 S_0
Metric =70	20.0.0.0/24 , 70 S_1

و RTG B ~ ~ ~

هنا بقى ال DUAL هتشتغل وهتحسب The best path & Back up path

← The best path [successor] (الطريق الناجح) وهنطلق الرمز دة S

← The Back up path [Feasible successor] ~ ~ ~ FS

منه بردوه

* متساش ان العمليه دى بتم فى ال Topology Table

وهنا بقى The Topology table هياخد Copy من Best path (successor)

وهيطبعها فى ال Routing table. A

الخطوة التاليه / Router A هيعمل Full RTG update لل Neighbor اللى حواليه

ولكن فى شرط مهم انه يشغل خاصيه split Horizon rule بمعنى [Router A

هيرسل لـ Router B كل ال RTG Table بتاعه ماعدا الحاجات اللى اتعلمها من

Router B نفسه]

الحمد لله خلصنا Start up

ملحوظه / ال Back up path موجود فى ال Topology table فقط

لكن ال successor موجود فى ال Topology table وال RTG table

---

[2] at convergence

* there is no periodic update as D.V protocols [RIP v1, IGRP]

* but there is periodic Hello to be sure that all Networks are keep alives [with dead time = 3 * Hello]

→ there are two types of interfaces Fast & slow interface
ودة بيعتمد على ال Technology

* Fast interface when speed > 1.54 Mbps
* slow ~ ~ ~ ≤ 1.54 Mbps

periodic Hello

every 5 sec for Fast Interface

∴ Dead time = 3 * 5 = 15 sec

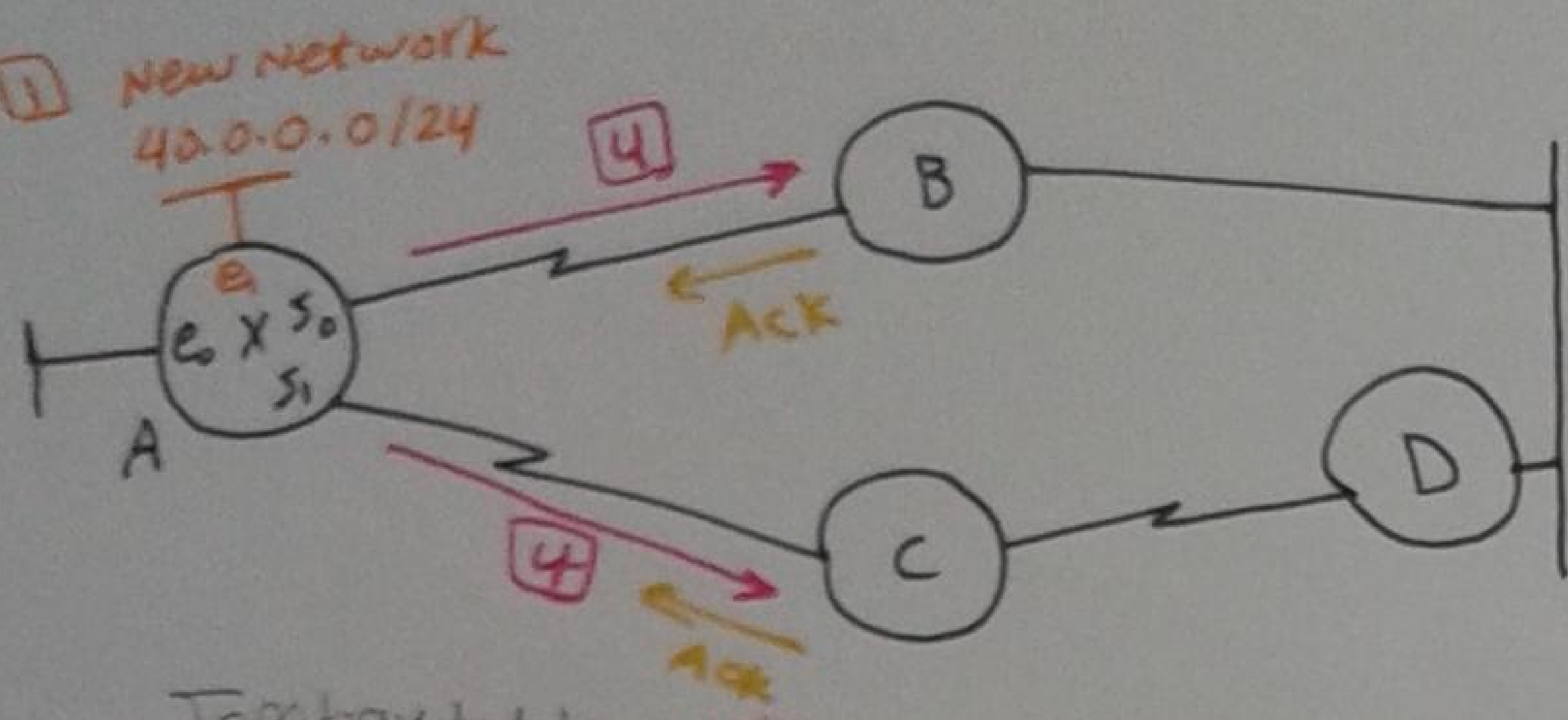
→ يعنى بعد الوقت دة هيعتبر ان الشبكه وقعت وهيحذفها من ال RTG Table

every 60 sec for slow interface

Dead time = 3 * 60 = 180 sec

3 at change

1 If new Network appears :-



Topology table — metric

2 C 40.0.0.0/24 10 e1 → S (successor)

3 copy in RTG table

RTG table

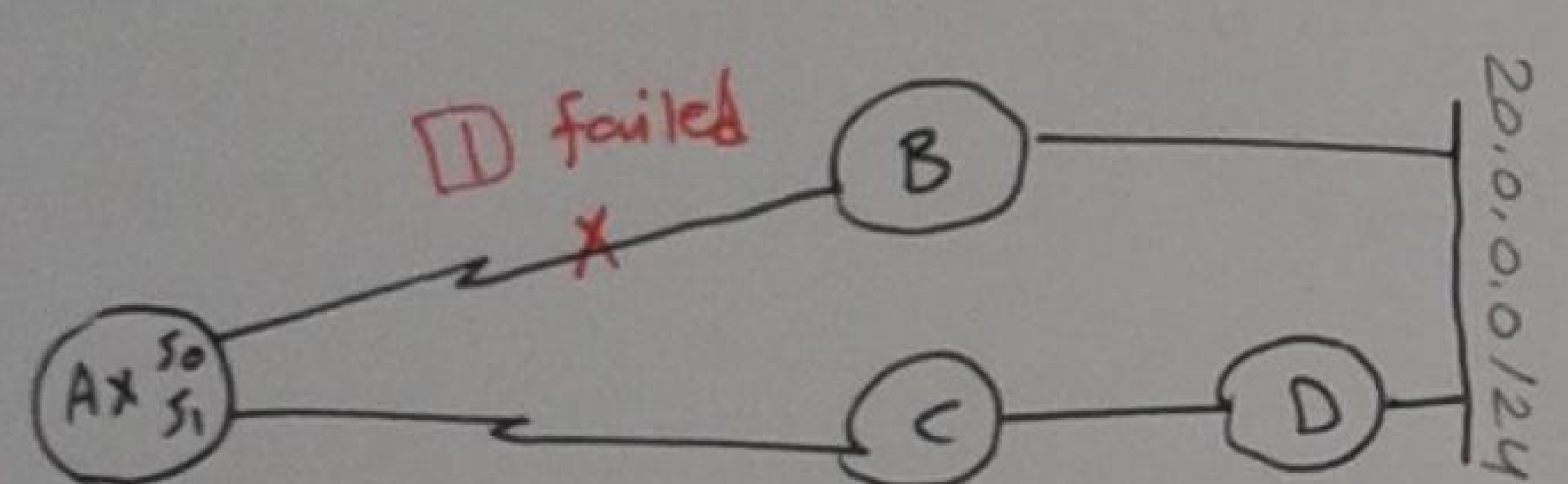
C 40.0.0.0/24 10 e1

4 send partial triggered update to neighbor
بمعنى انك هتبعت التعديل الى حصل (الشبكة الجديدة)
لـرطيا الـ neighbor [Router B&C]

5 ⟶ Ack

---

2 If route fails & there is Back up [FS]



Topology table

2 ~~20.0.0.0/24 30 S0~~ → S
20.0.0.0/24 70 S1 → FS

3 copy to RTG Table

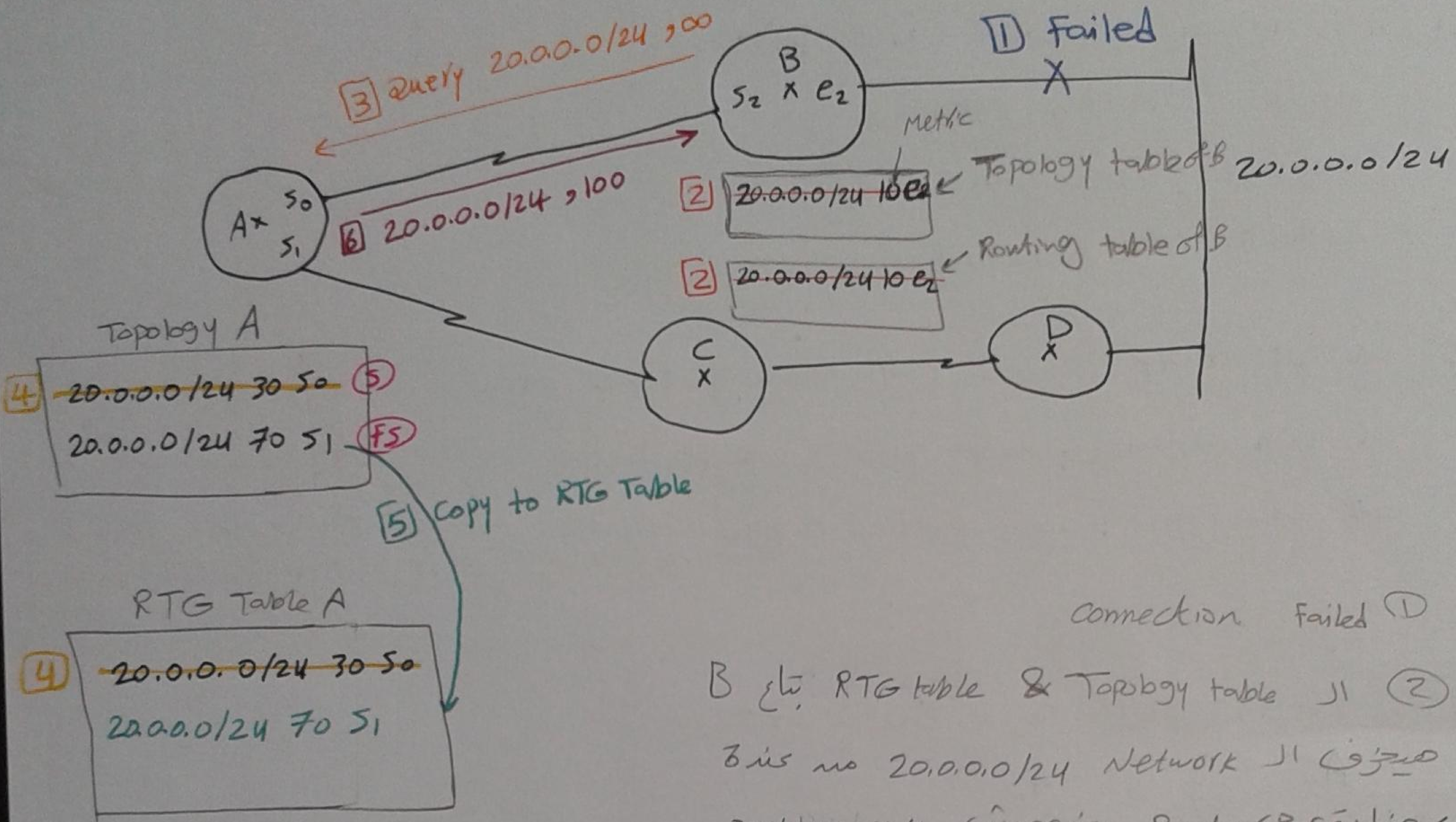
RTG table

2 ~~20.0.0.0/24 30 S0~~
20.0.0.0/24 70 S1

4 send partial triggered update to neighbor

① Connection failed
② هحذف 20.0.0.0/24 30 من
الـ Topology table & RTG Table
فى نفس الوقت
③ هاخد copy من الـ pack up path
فى الـ Topology table وسارسله الى RTG Table
④ سوف ارسل partial triggered للـ neighbors
لكن بما انى مشغل خاصيه الـ split horizon ،
مش هينفع اعلم لـ Router C السطر 20.0.0.0/24 70 S1
عشان انا اصلا واخدها منه

3 If route fails & there is no FS



① Connection failed

② ال Topology table & RTG table بتاع B
هيحزف ال Network 20.0.0.0/24 من عنده
← هنا بقى Router B معندوش pack up path
فى ال Topology table

هو المفروض يبعت ال Query لكل
ال Neighbors اللى متوصلين بيه

③ Router B هيبعت لـ Router A سؤال
بيقوله فيه انه $\overset{32bit}{\infty}$ و 20.0.0.0/24 [بمعنى
انه ال Network دى وقعت من عندى وعايز
اى طريق تانى ليها] ملحوظة ∞ عبارة عن
32 bit كلهم وحايد [1111...1111]

④ Router A هيحذف 20.0.0.0/24 30 S0 من
عنده فى ال Topology table و RTG Table

⑤ وهيعمل copy لل 20.0.0.0/24 70 S1 (Backup path)
من Topology table الى RTG table

الخطوتين 6 & 7 بيتموا مع بعض

⑦ هيرسل partial trigger replay
to neighboor

وكالعادة مش هيمشى تحت عشانه خاصية ال split horizon وهيمشى فوق عند Router B

⑥ Router A هيحسب ال Metric الجديد بتاع 20.0.0.0/24 70 S1 وهيرسله
لـ Router B [20.0.0.0/24 100 S2]

ملحوظة / ال Query بيذهب الى اقرب Router خلال 0.1 sec ← سريع جداً من RIPv1

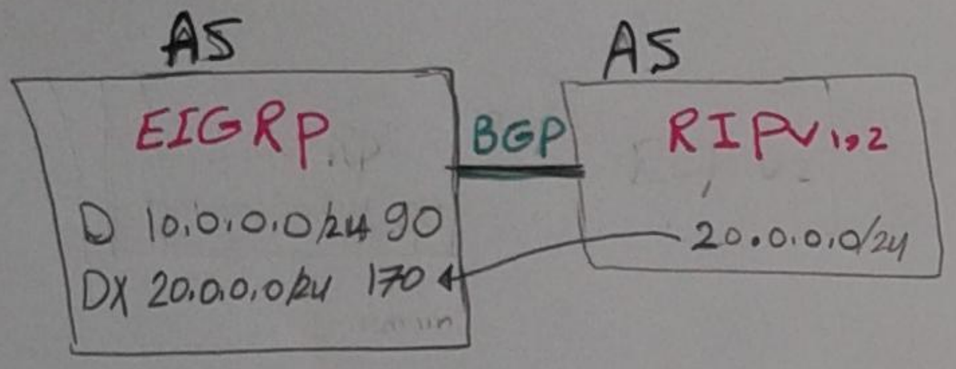
* EIGRP C|C's

[1] it is advanced D.V Cisco protocol
- MASK [classless protocol]
- Multicast [use 224.0.0.10]
- Authentication password [optional]

[2] at start up: send full Routing table once
at convergence: only send 3 periodic Hello
at change: send partial triggered update → If S fails, use FS
→ If S fails, no FS → send Query

[3] symbol in Table "D"

[4] admin distance = 90 & 170



لو 20.0.0.0/24 عايزة تكلم 10.0.0.0/24
اولاً BGP صيحولها من (BGP ← RIP)
ثانياً BGP ~ ~ (EIGRP ← BGP)
وميأخدها EIGRP ، ميكلمها Metric = 170

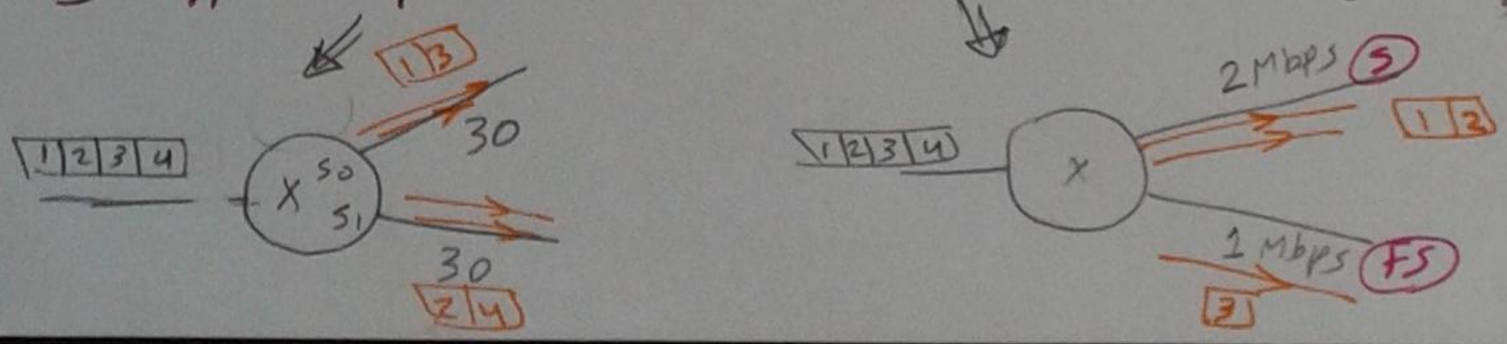
[5] EIGRP Metric (32 bit) = 256 * IGRP Metric (24 bit)
{ BW , delay , load , Relaiability , MTU }
default

max no of hops = 224

[6] use DUAL to calculat best path & back up bath

[7] support many routed protocols [IPV4 , IPV6 , IPX , Apple talk]

[8] support equal & no equal loadsharing [4 paths by default , max [16 or more]]



لاحظ انه بقدر يبعت على طريقين
الطريقين مع بعض

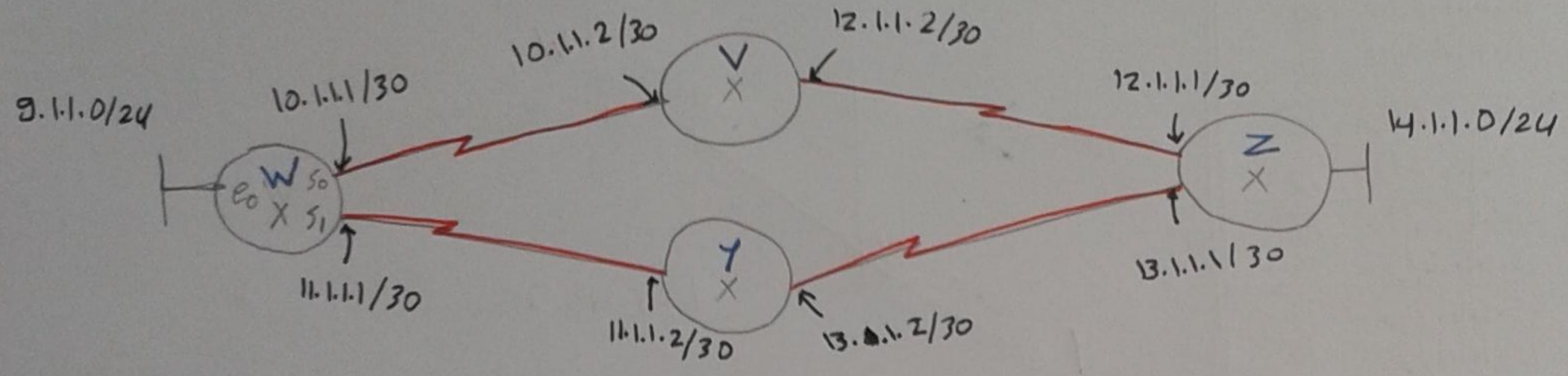
link state

ex : OSPF (open shortest path First)

ISIS

ليزلت [1] D.V [2] link state [3] advanced D.V

∞ EIGRP is Hypred of RIPv1 & link state



[1] at start up (we assume that Explanation about Router W

(config if) # router ospf

(config Router) # Network —

[A] neighbor discovery (exchange of Hello)

→ to produce neighbor table

↳ Hello is sent broadcast

Ip of neighbor	Interface
Ip of V	S0
Ip of Y	S1

[B] Route discovery (exchange of updates) ⟶ is sent multicast

↳ LSAs

Each router will form a packet discribing itself called LSA " link state advertisment] and send its LSA to all neighbors

Network / mask	Metric	
9.1.1.0/24	10	Router ID
10.1.1.1/30	10	W
11.1.1.1/30	10	

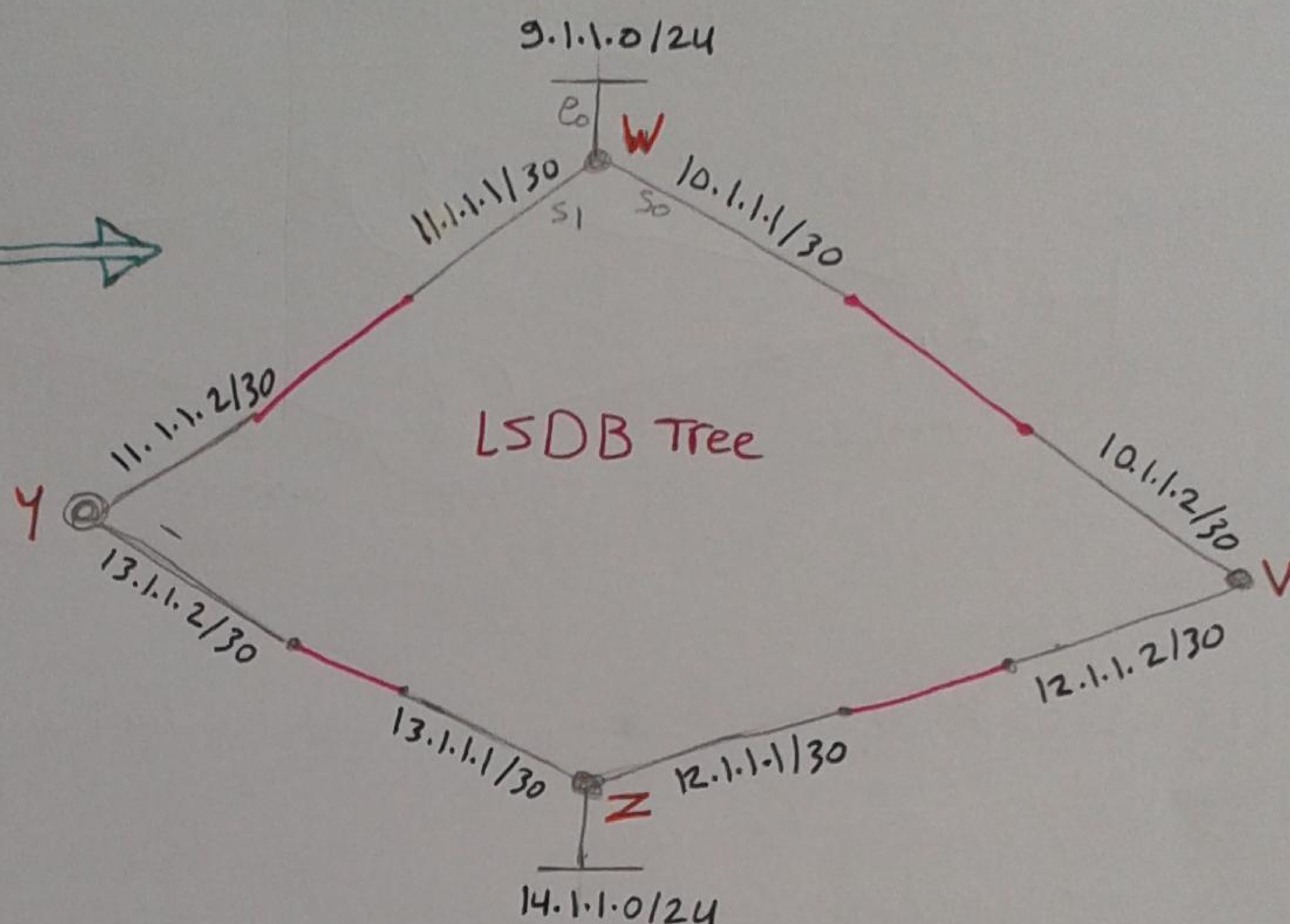
⟹ LSA of W

[C] Each Router that receives LSA will talk a copy of it in its LSDA " link state Data base " and send another copy of LSA as it is to all other neighbors

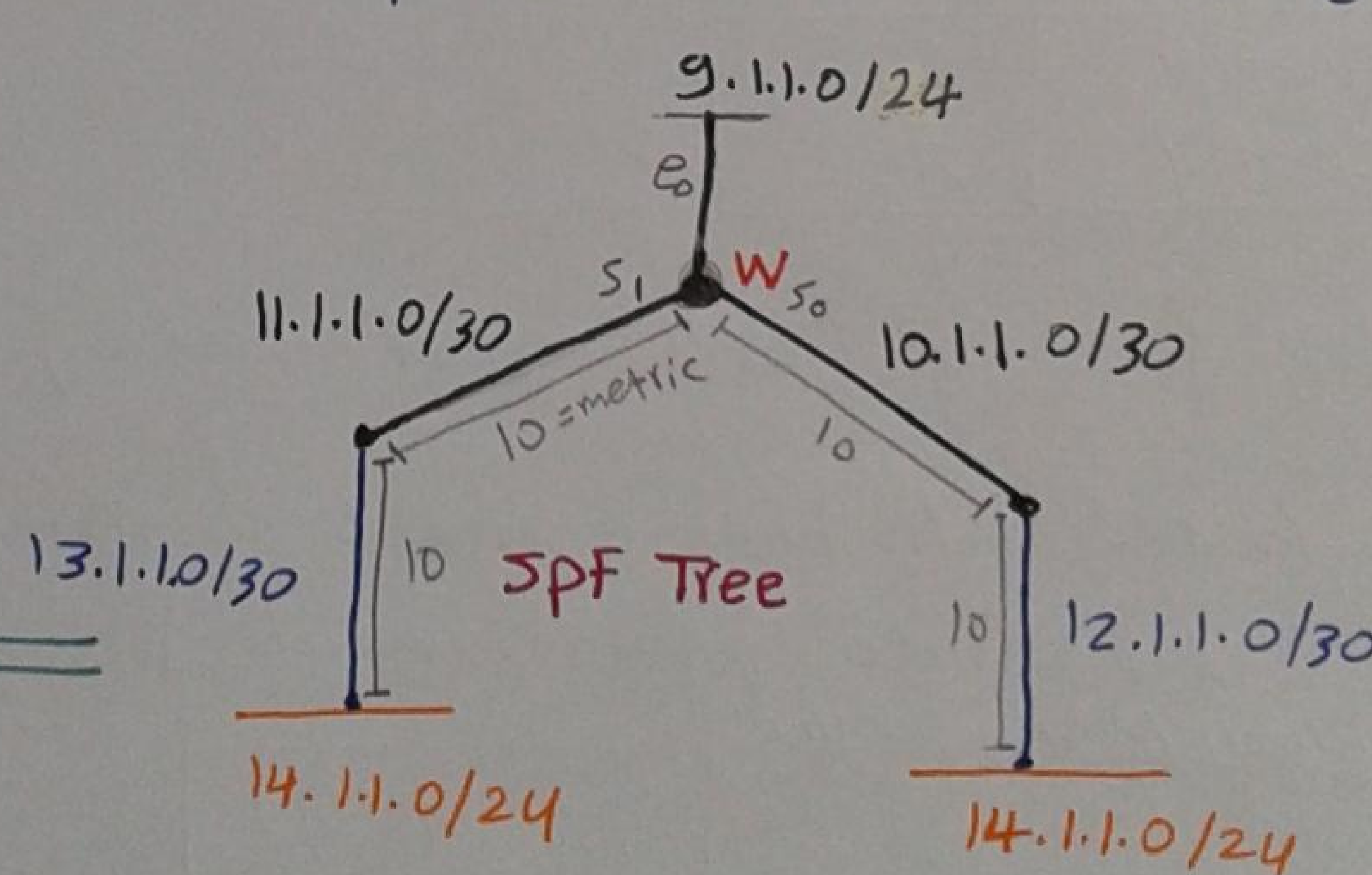
LSDB (a group of LSAs)

	network/mask	metric
W	9.1.1.0/24	10
	10.1.1.1/30	10
	11.1.1.1/30	10
V	10.1.1.2/30	10
	12.1.1.2/30	10
y	11.1.1.2/30	10
	13.1.1.2/30	10
Z	12.1.1.1/30	10
	13.1.1.1/30	10
	14.1.1.0/24	10

Note / I take in consideration split horizon



Dijkstra algorithm
SPF [shortest path first] algorithm



RTG table of W

9.1.1.0/24	e0	0
10.1.1.0/30	S0	0
11.1.1.0/30	S1	0
12.1.1.0/30	S0	10
13.1.1.0/30	S1	10
14.1.1.0/24	S0	20
	S1	20

* عشان اعمل SPF Tree من LSDB Tree
هنفذ run 6 process times

* ممكن اعمل load sharing لـ network
رقم 14.1.10/24 من الرسمه

2 at change

Router that Feels change will send New LSA discribing its current State triggered to all neighbors

LSA

10.1.1.1/30	10	Router ID
11.1.1.1/30	10	W

① لو 9.1.1.0 وقعت ←

② كل Router هيشيل LSA القديمه ويضع الجديدة

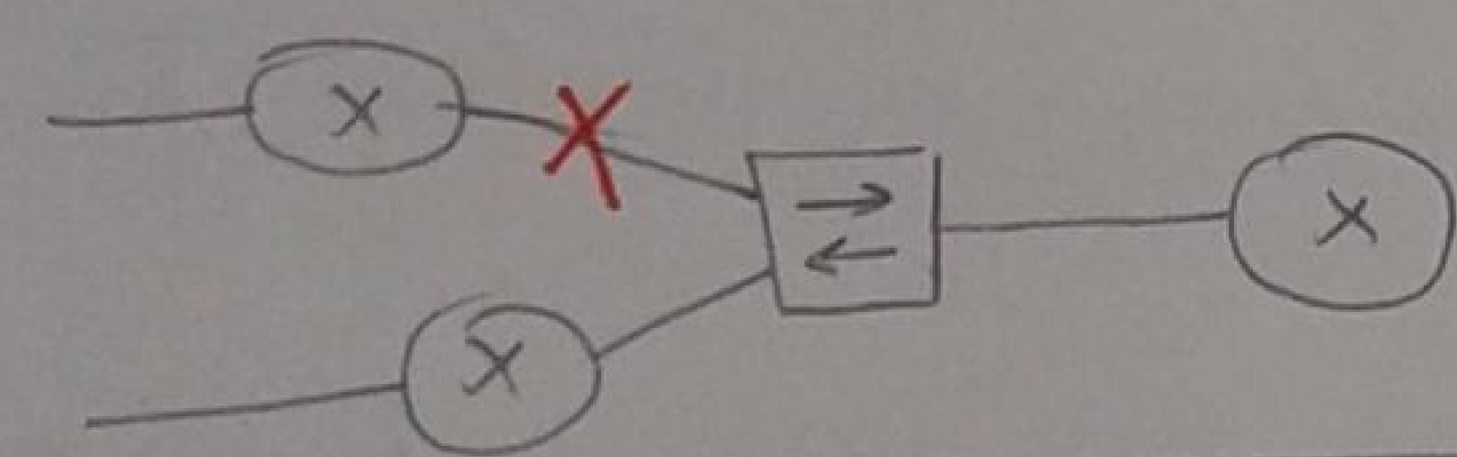
③ كل 20 Router بياخدوا 5 secs للـ process ، يعني في بعض الـ networks الصغيرة محتاجين 5 sec بس عشان يرجع الـ Convergence تاني

3 at Convergence

A send periodic Hello every 10 sec [Hello for 4 times]

B send periodic LSA every 30 minute
it is sent as LSDB refreshment

يعني لو روترين متوصلين ببعض point to point ، لو واحد وقع التاني هيحس بيه في نفس الوقت. لكن المشكلة لو أكتر من Router متوصلين ببعض point to Multipoint لو واحد وقع الباقي مش هيحسوا بيه ، عشان كدة انا بستخدم perodic LSA ثابتة كل ½ ساعه



---

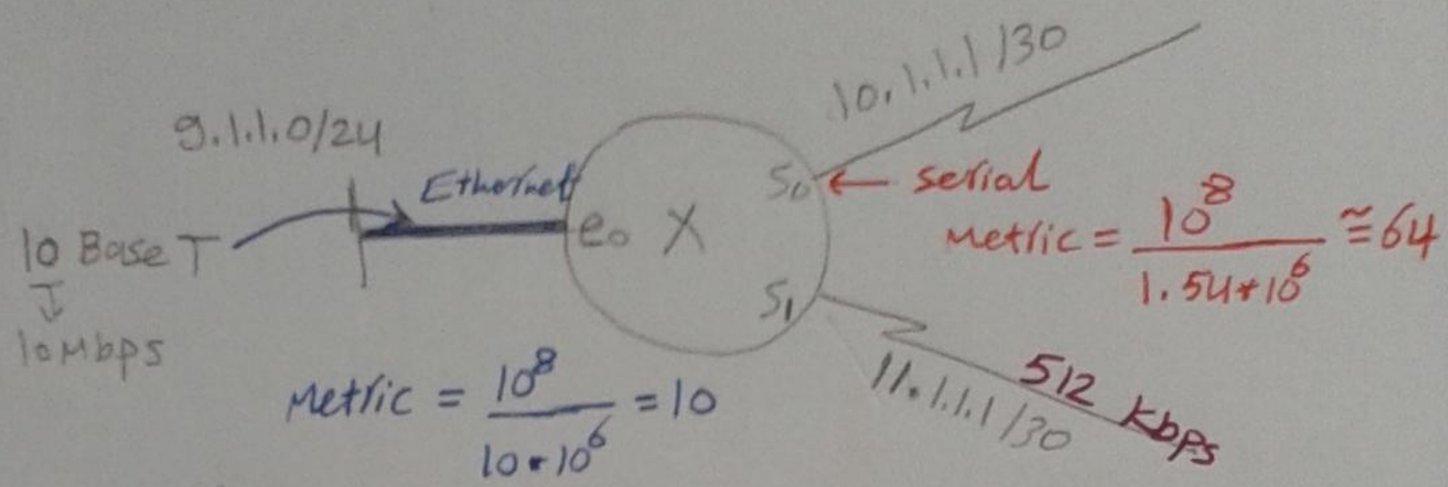
ospf ch/c's

1- it is open standard → every one can develop in it
2- Mask [Class less protocol]
3- Multicast [use 224.0.0.5 & 224.0.0.6]
4- Authentication (option)
5- use Dijktra algorithm
6- symbol in Table "O"
8- admin distance = 110

9- metric ≡ cost = $\frac{10^8}{\text{Bandwidth}}$ [default for serial = 1.54 Mbps]

LSA for W

9.1.1.0/24	10	W
10.1.1.1 /30	64	
11.1.1.1 /30	64	



the defaut / the router set any serial port by metric 64 [defaut], unless you set the speed by yourself with this order (config-If)# bandwidth 512 (in units of kbps)

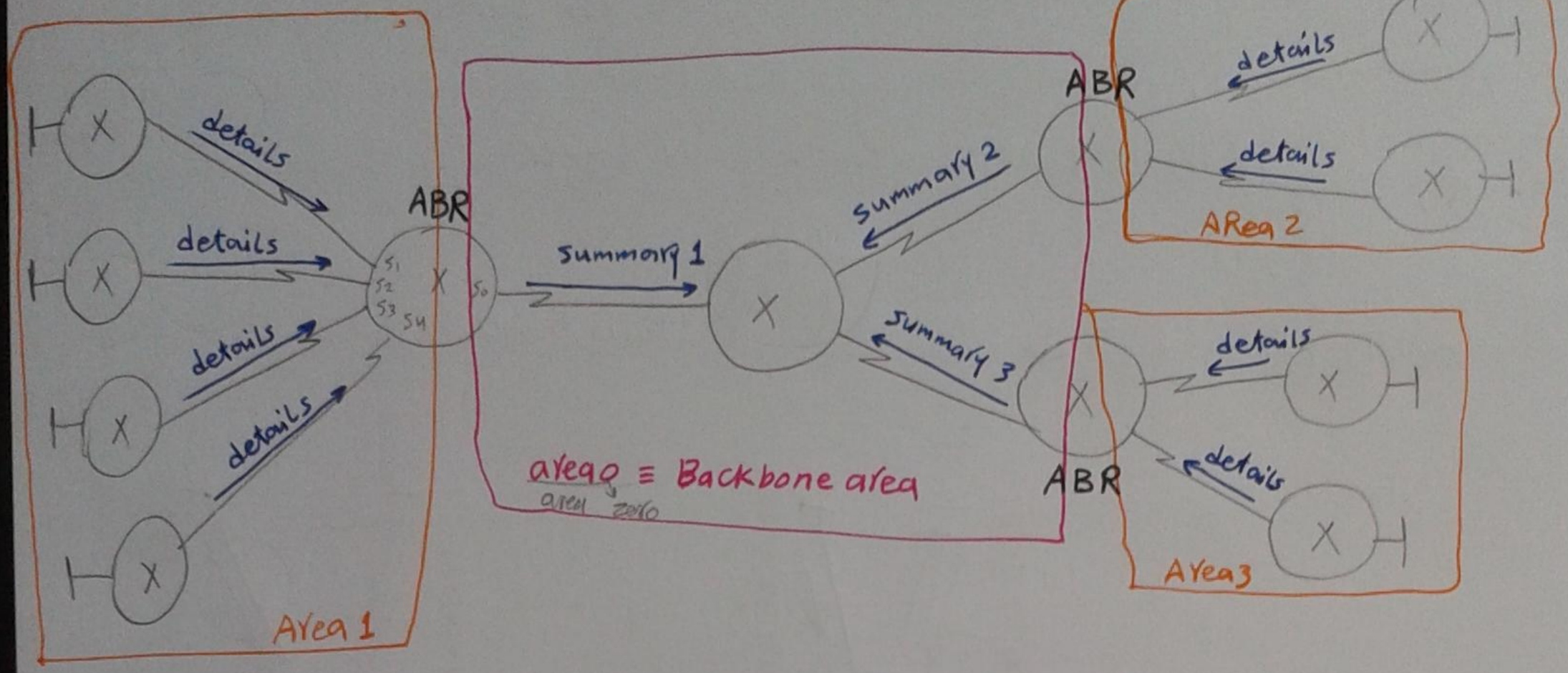
10- Hierarchical design (multiple access ospf)

* before Hierarchical design

1. need high processing
2. need big memory
3. instability affect intire AS (Autonomos sys.) (as Flapping الرفرفه)
4. Complex [design, Implementation, configuration]

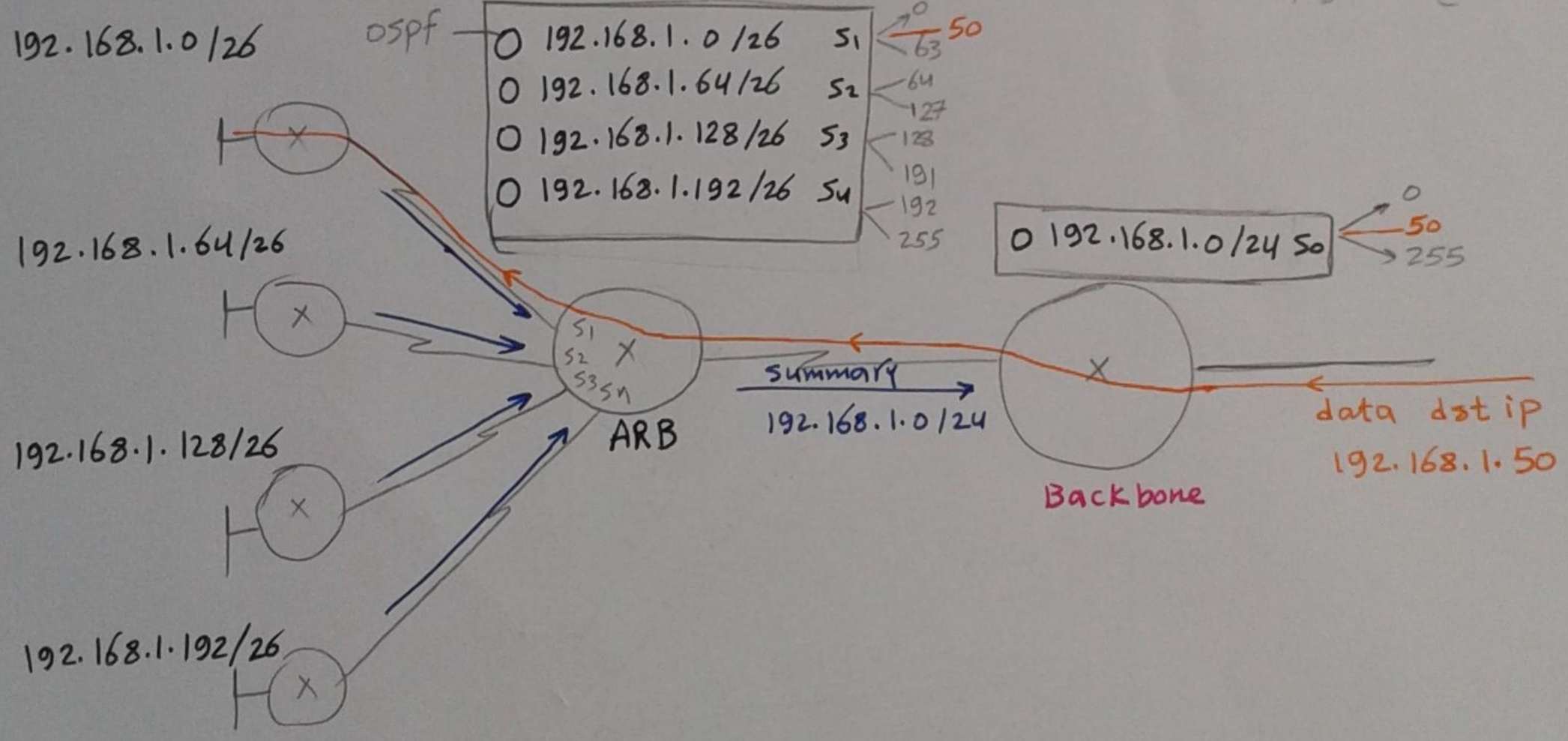
The solution is :- Deviding AS into sub ASs called Areas (If no of Routers > 50)

Area :- Each area contain and know all details about Routers in that area and summary only about other areas.



ABR : Area Boarder Router / it is responsible for taking details from all interfaces and outcome the summary of one interface

* انت رتبت الروترات اوى بكده الـ Design هيكون complex بالنسبالك وانت بتنظم الـ IPs



Note Home Router

0.0.0.0/0 ⟶ H=32

∴ 2^{32} = all

* Route summarization & CIDR [Classless Interdomain Routing]

* Route summarization / grouping subnets and advertise them as single Major Network
* supernetworking / grouping Major networks and advetrise as supper network (CIDR)

Common الـ جميع من → common ⇒ /25

192.168.1.128/26
192.168.1.192/26
⇒ 192.168.1.1 000 0000
192.163.1.1 00 0000
→ 192.168.1.128/25

* In RIP v2 & EIGRP

⟹ by defaut auto summary in them

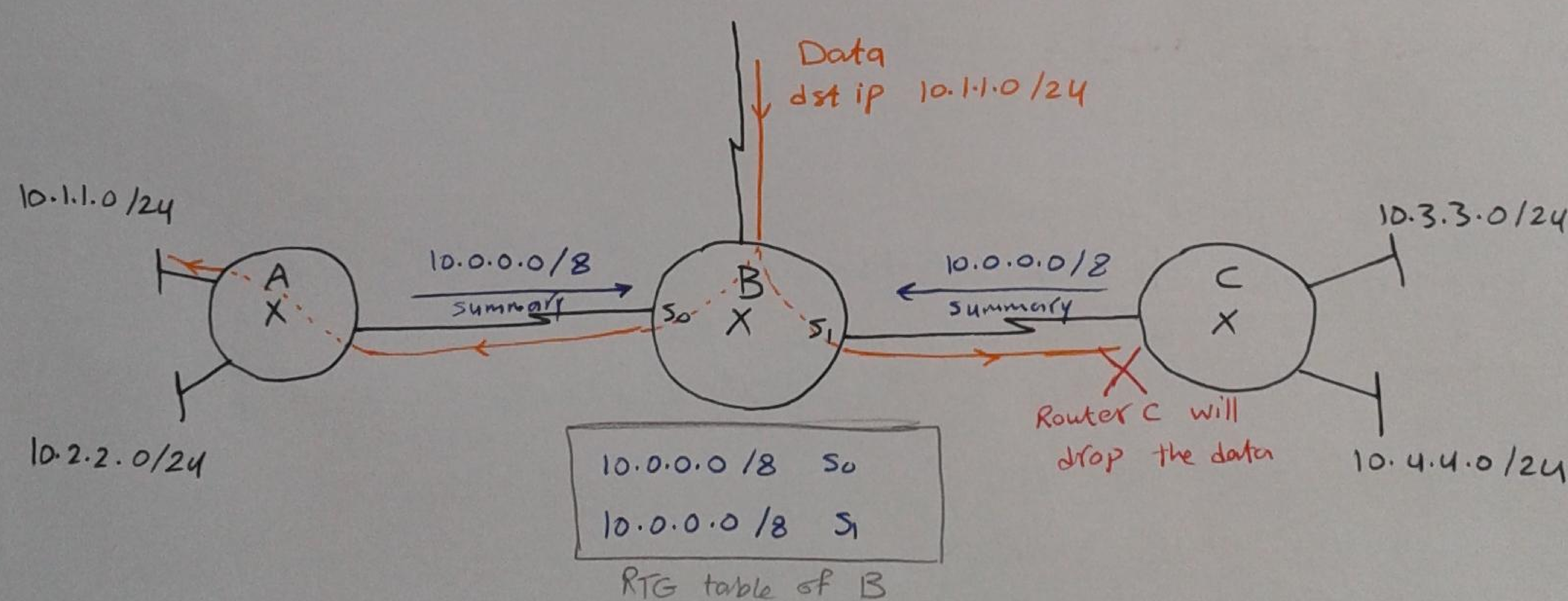
[الشكله اللى هتحصل هنا اسمها discontiguos network]

* لو ال Router وجد اكتر من Network بتبدأ بعنوان ثابت ، ال Router بينظر لاول octet من العنوان ده و بيحدد (class A / class B / class C) ، وعلى اساس نوع ال Class بيضع ال Mask ، لكن المشكله زى الرسمه وهى ان Router A عليه interfaces متوصلة بـ 10.1.1.0/24 & 10.2.2.0/24 ⟸ Router A هيعتبر انها class A وهياخد summary ال Mask ⟸ 10.0.0.0/8 و Router C نفس الوضع هياخد summary بنفس ال Mask واسم ال Network

⟸ هييجي Router B وهيعرف ان عنده 10.0.0.0/8 متعرفه على 2 interfaces (S0, S1)
وبالتالى لو ذهب له dst IP 10.1.1.0/24 هيعتبر ان ال 2 interfaces بيوصلوا لنفس ال distination وهيعمل load sharing ويضيع جزء كبير من ال packets

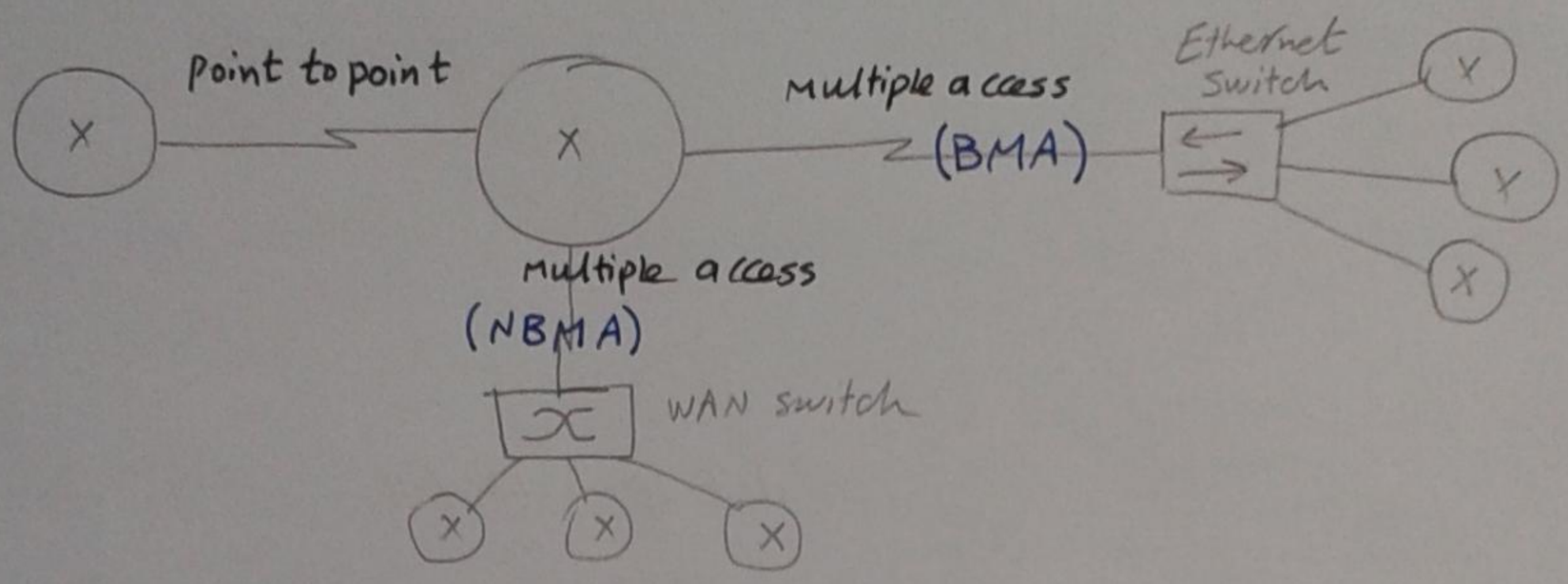
⟸ حل المشكله دى انك هتلغى خاصيه ال auto-summary بالامر ده

(config-router)# no auto summary



* ospf topologies → point to point
→ point to multipoint [Multiple access]

* Multiple access → BMA [Broadcast multiple access] used in LAN
→ NBMA [non Broadcast multiple access] used in WAN
يعني انه مفيش Broadcast في الـ WAN

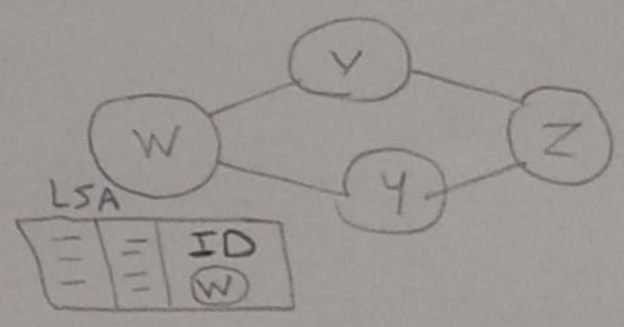


---

* OSPF operation in Multiple access

at start up : (config) # Router ospf #

[1] Router ID [RID] : 32 bit
الافضل انه يكون private



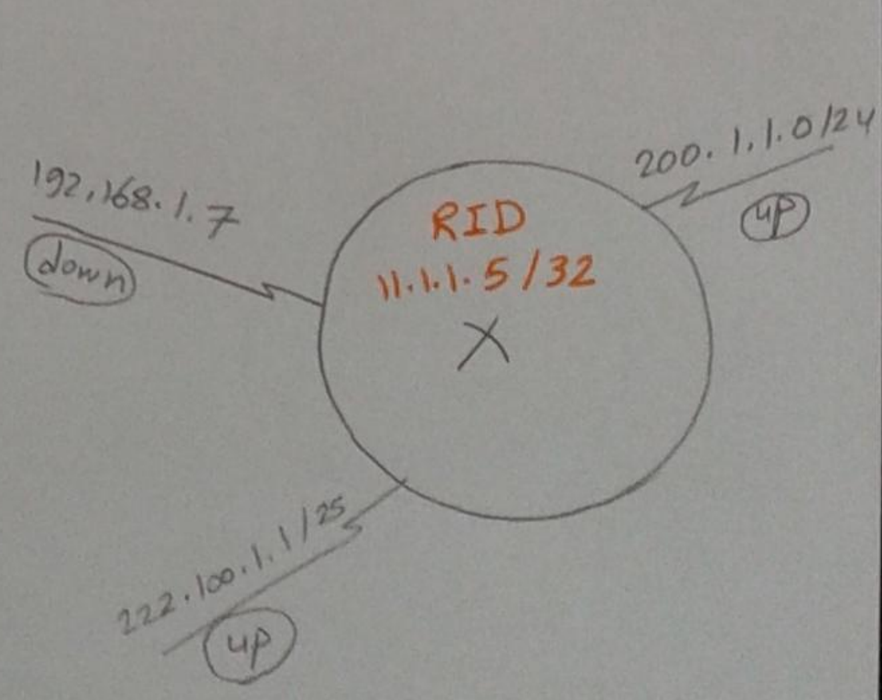
② it is the highest IP address configured on loop back Interface

internal s/w logical vertual always up → means no shutdown
يعني انه لو الجهاز اتطفى و اتفتح تاني
مش بيتمسح من الجهاز

* you introduce ID Manually
* adv. → it is more stable
الأمر

(config) # interface loopback 0
غيره بأي رقم

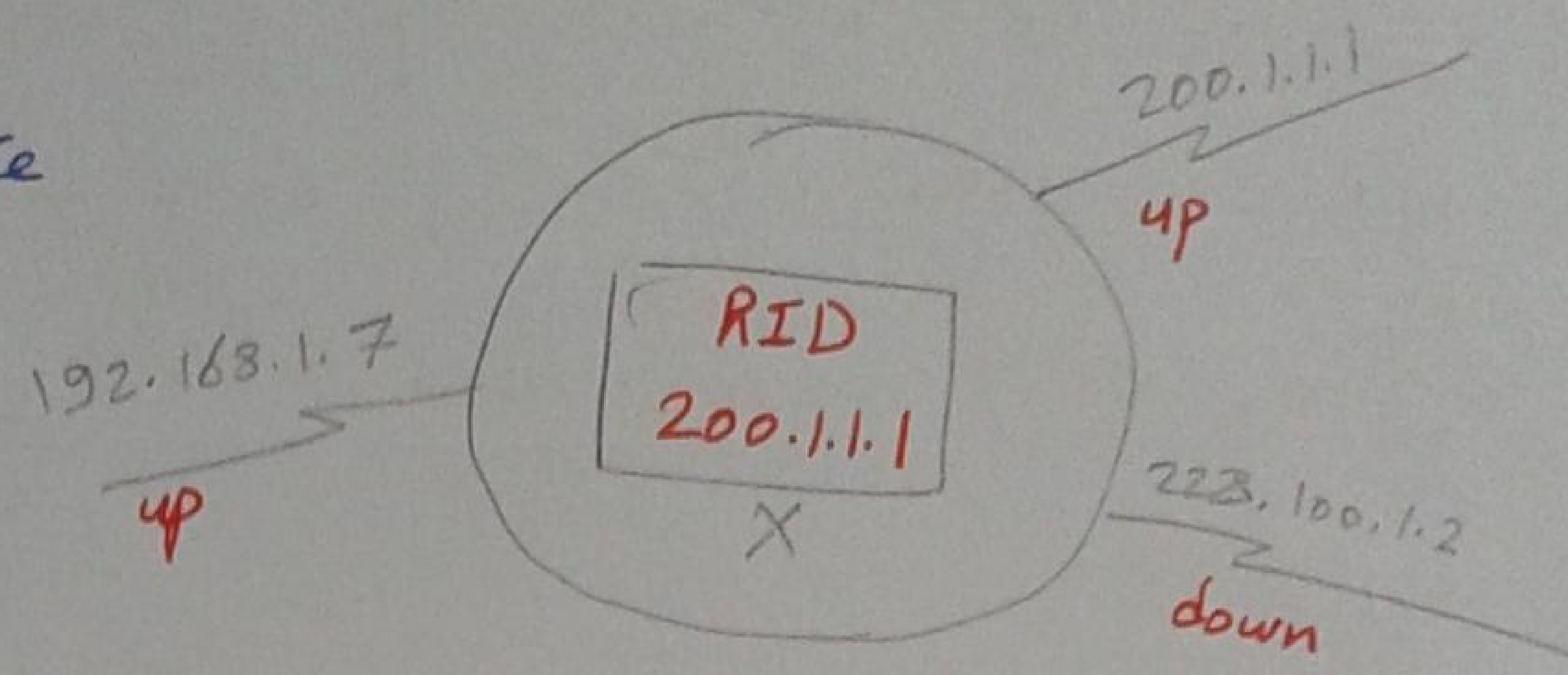
(config-If) # ip address 11.1.1.5 255.255.255.255
ID Host Mask



Note/ Mask → /32 ∴ H = 0
∴ no of IPs = $2^0 = 1$
∴ this IP is the only on of his subnetwork → we don't wast IPs
Home Router
لازم انه دي تفضل فاضية و الـ IP بتاع الـ

(b) it is the heighest IP address configured on physical active interface

physical → Ethernet / serial

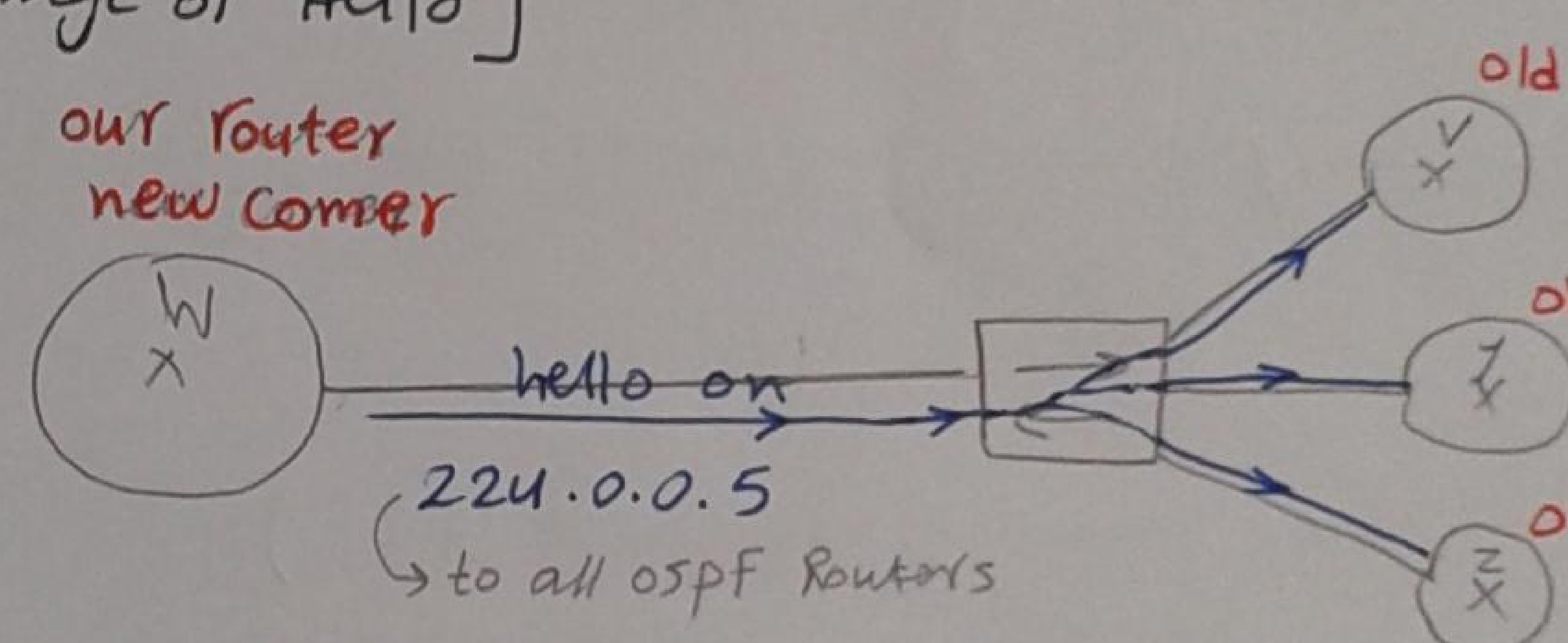


* وهنا اول ما ال Router بيفتح. بينظر الى كل ال Interfaces (Ethernet or serial) اللى عليه [up] وبعدين هيشوف
اكبر IP عنده وياخده كـ (ID) لنفسه وال ID ده بيكون ثابت للـ Router
حتى لو ال Interface دى فصلت (Down) طول الوقت (الا فى حالة) ال Router كله
فصل وساعتها هيبدأ من جديد يدور على اعلى IP [up] وياخده ID جديد لنفسه

ملحوظة/ اول حاجه بيعملها ال Router عشان ياخد ID هو انه يدور الاول على loopback interface
ولو ملقاش هيدور على اكبر IP serial interface عنده وهياخده ID

2 Neighbor discovery [Exchange of Hello]

* hello is sent Multicast to all neighbors on this IP [224.0.0.5]
; The routers that configured OSPF protocol can only receive this multicast IP [224.0.0.5]



The neighbors of new router won't receive the hello msg Except with these conditions :-

1. Authentication passord [password]
2. Same area to be sure that the new router is our neighbor
3. same hello interval = 10 sec [defaut] but it can be changed by configurati
4. same dead interval = 4 hello = 40 sec

لكن المشكلة هنا ان لما Router W يبعت Hello لـ Router V, Y, Z هيبتدولوا LSAs
يعنى router W هيستقبل 3 LASs متكررين ← المشكلة ان العمليه دى هتشغل
ال processor اوى وهتملى ال Memory على الفاضى عشان كدة كان الحل
فى DR (الرئيس) و ال BDR [نائب الرئيس]

[3] Routes Discovery [Exchange of LSAs]

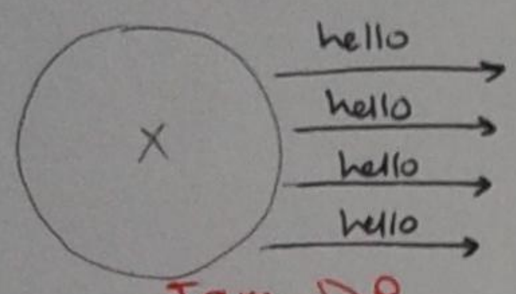
before Routes Discovery there is the electing of DR & BDR

الروتر المسؤول (الريس) — نائب الريس

[2] Electing Designated Router [DR] & Back up DR [BDR]

DR is

[a] first router to boot ospf with enough time



(40sec) 4 hello لو مفيش حد رد بعد
هيقول انا الريس

← لو فى 2 Routers قاموا فى نفس اللحظه هنروح لخطوة [b]

[b] Router having hieghist periority on interface

* periority (0 – 255) the higher the number, the higher the periority
* The periority in all Routers = 1 (by default), you can change the periority by configuration
* periority 0 ⇒ can never be DR or BDR, and it will be [DR other]

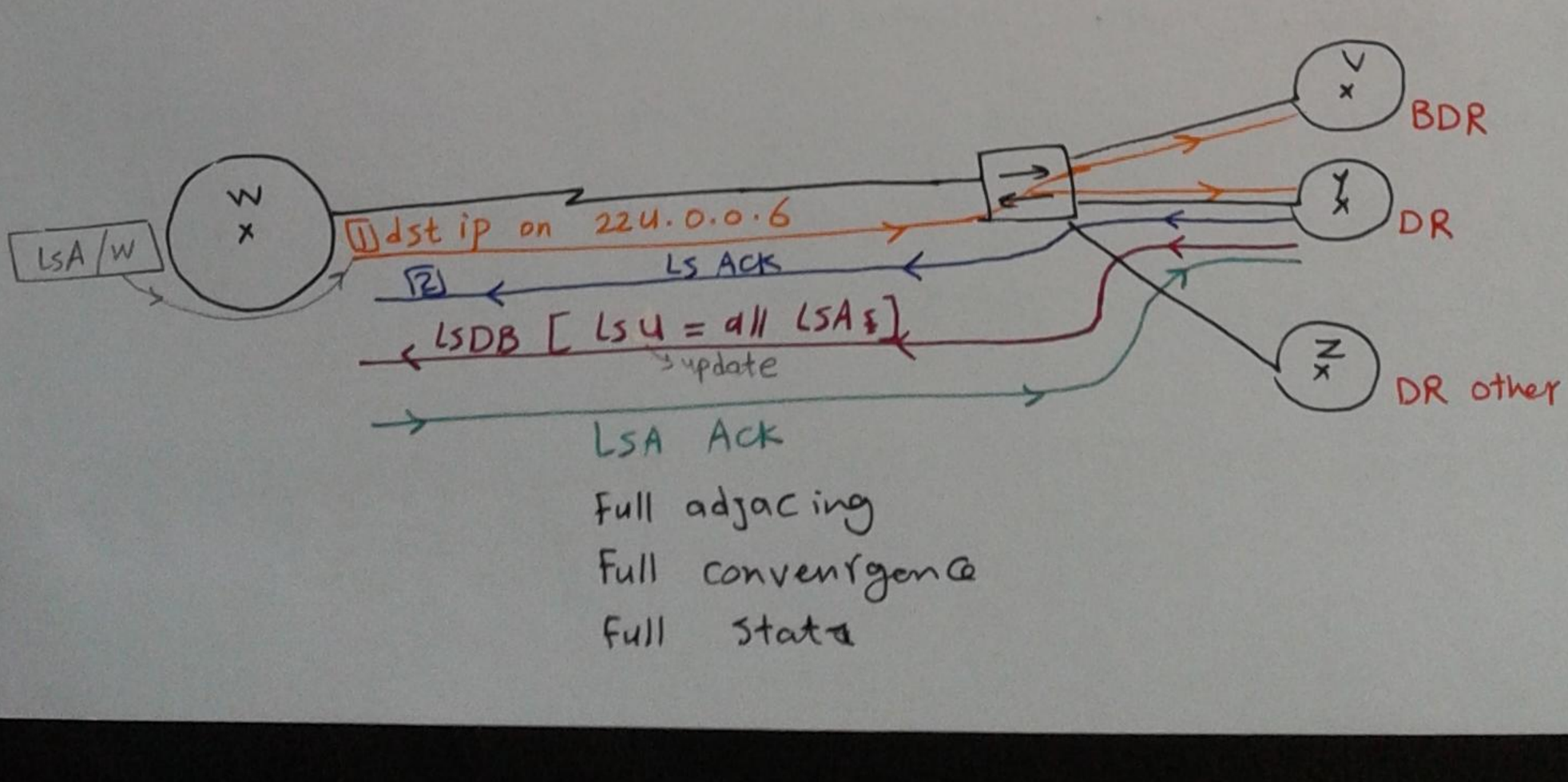
← لو اكتر 2 Routers لهم نفس الـ periority هنروح لخطوة [c]

[c] Router having highest (RID)

* مش معنى انه Router له اعلى RID فانه افضل واحد لكنه لازم يعمل كده عشان نشتغل

224.0.0.5 → to all neighbors to say Iam a live
224.0.0.6 → to DR & BDR only

الاتنين بيبعت عليهم Hello MULTI cast ←

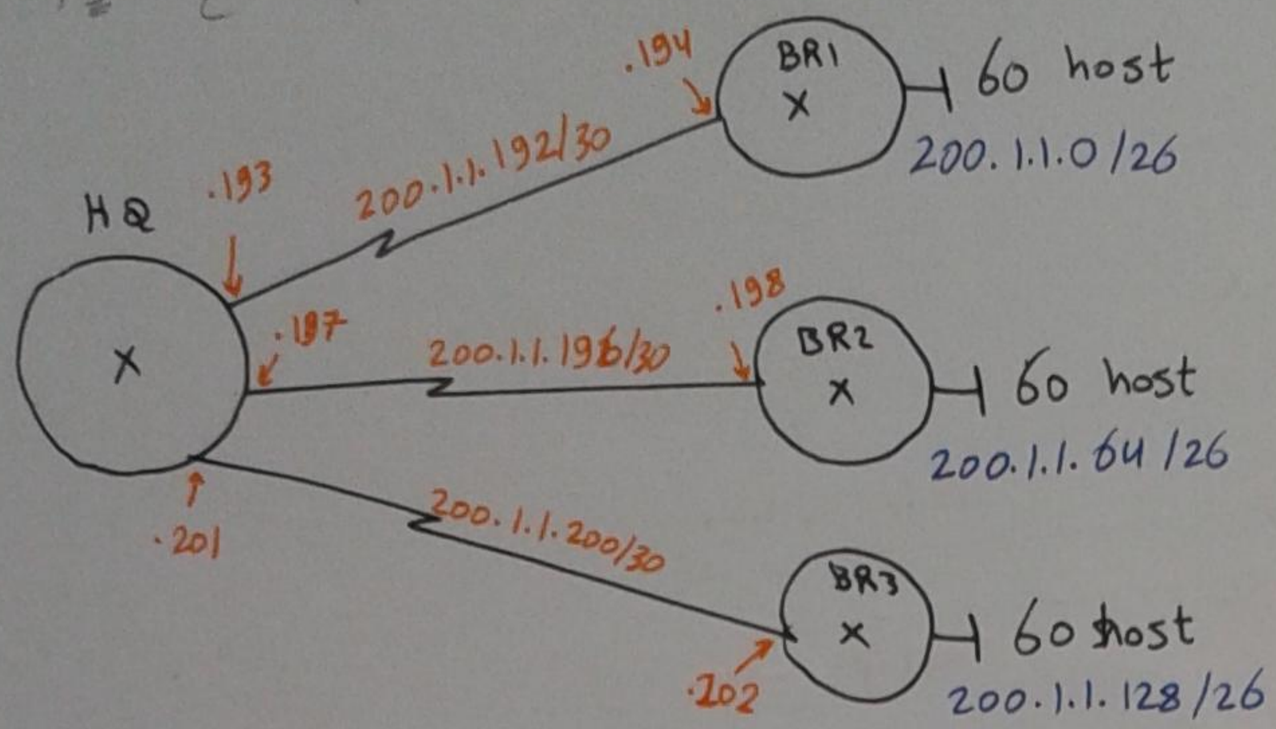


Full adjacing
Full convenrgence
Full state

BR : branch
HQ : Head Quarter

* VLSM [Variable length subnet mask]

انت عندك 200.1.1.0/24 وعايز تقسمهم وتوزع الـ IPs



* انا محتاج كام IP

(60+2)
+(60+2)
+(60+2)
+(2+2)
+(2+2)
+(2+2)

198 IP

* انت محتاج 3*62 IP ⇐ هتشوف اقرب Host حساب يعطيك اقرب رقم من 62IP

08 H=6 ⟹ no of IPs = $2^H = 2^6 =$ (64 IP) → مناسب جدا

hoppa

↳ H=6 ، ∴ N=26

200.1.1.0/24

200.1.1.0(hoppa)/26 — 200.1.1.0/26

200.1.1.1*(hoppa)/26 — 200.1.1.64/26

200.1.1.2*(hoppa)/26 — 200.1.1.128/26

200.1.1.3*(hoppa)/26 — 200.1.1.192/26

* you want 3*4 IPs ⟹ (4 IPs) ⟹ $2^H = 2^2$ ⟹ H=2 ⟹ N=30

hoppa

200.1.1.(192+0*hoppa)/30 — 200.1.1.192/30

200.1.1.(192+1*hoppa)/30 — 200.1.1.196/30

200.1.1.(192+2*hoppa)/30 — 200.1.1.200/30 ------

Q: which Routing protocols can support VLSM & CIDR ???

Ans :- classless protocols حاجه بتقوم Mask يعني بتبعت Mask في الـ update [RIPv2 , EIGRP , OSPF , ISIS , BGP]

في نفس الـ AS — بين AS مختلفين

ماعدا [RIPv1 , IGRP] ← classfull مبيقوش Mask

* New Subnetting standard بيبقى فيه الامر ده [enable by default] ← (Ip subnet-0)

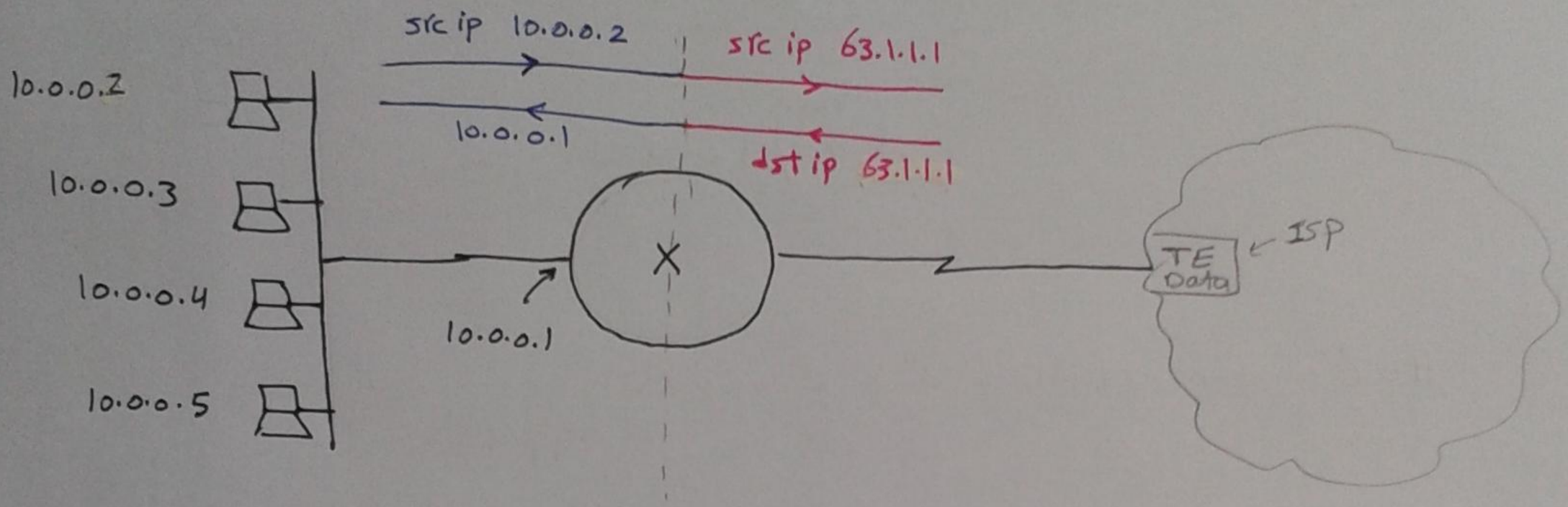
* old Subnetting standard بيلغى الامر بكلمة (no) (no Ip subnet-0)

↳ بتسبب اول واخر subnets لـ future

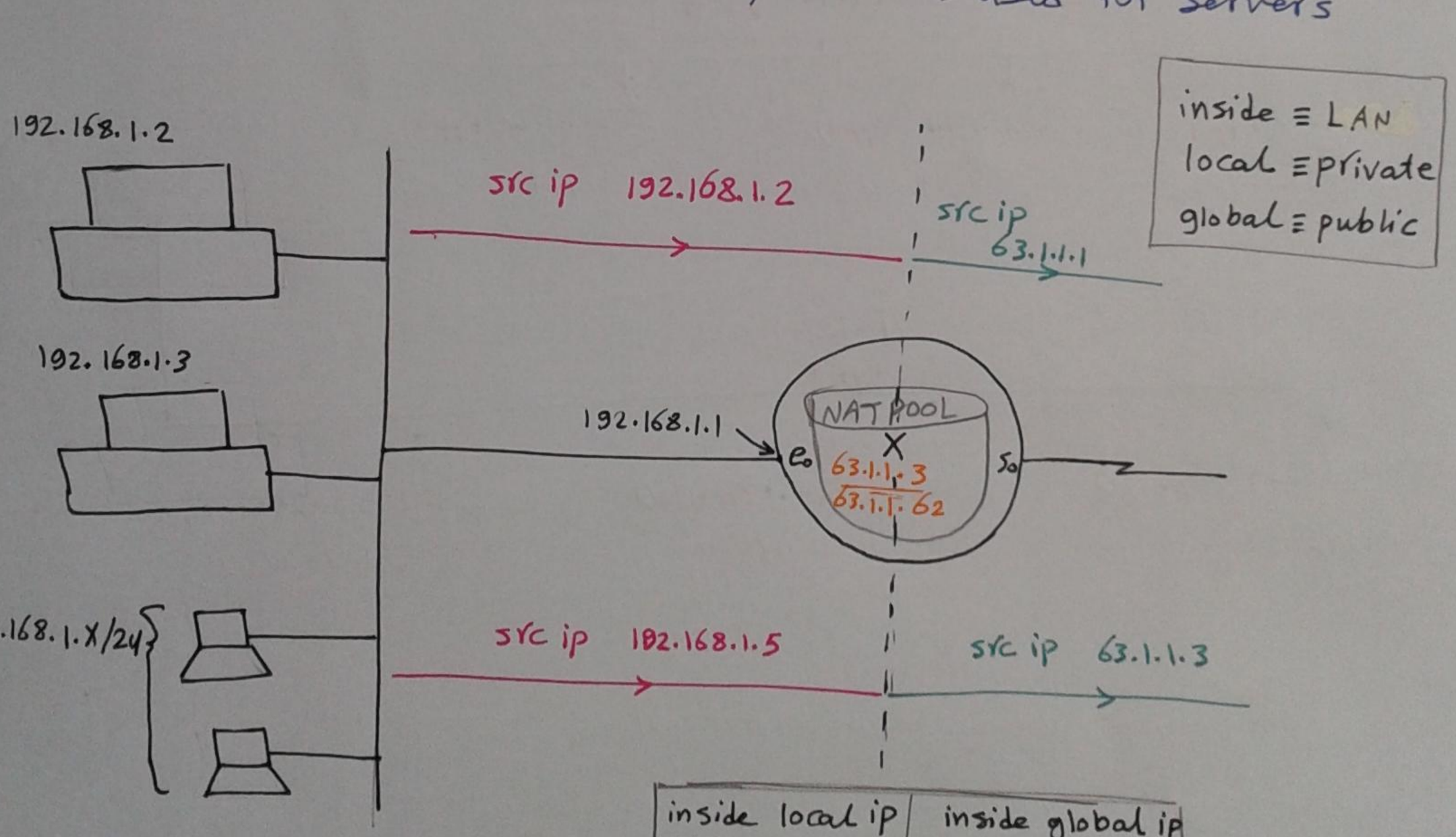
* NAT [Network address Translation] ISP : internet service provider

private IPs :-

10.X.X.X
172.X.X ⟶ 172.31.X.X
192.168.0.X ⟶ 192.168.255.X



1] Static NAT : 1 private ≡ 1 public ⟶ used for servers



inside local ip	inside global ip
192.168.1.2	63.1.1.1
192.168.1.3	63.1.1.2
192.168.1.5	63.1.1.3

* ملحوظة / ال servers مفيهاش توفير في IPs لأن ال server لازم يكون له IP ثابت ومعروف ، بالنسبه لو PC عايز يدخل النت بياخد اى IP من ال (NAT pool) ويدخل بيه وانا هنا بفترض انه مش كل ال PCs هتدخل على النت في نفس الوقت

ال PC اللى هيظل 5 min مدغير ما يدخل على حاجه جديدة ← ماخد منه ال IP بتاعه واحطه في NAT pool

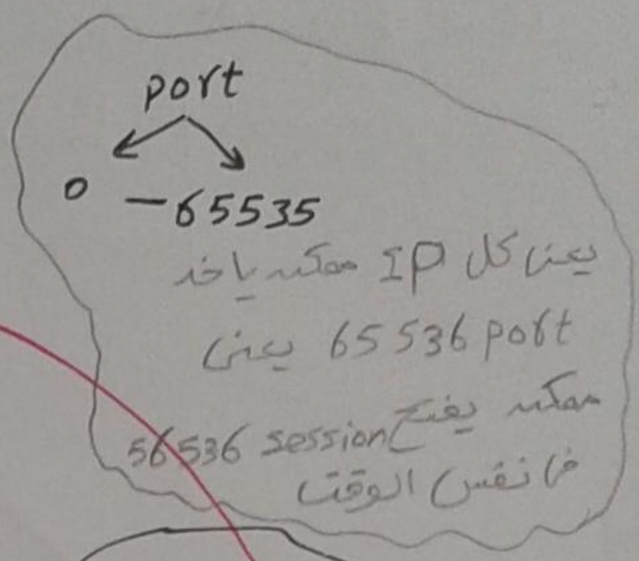
[2] Dynamic NAT

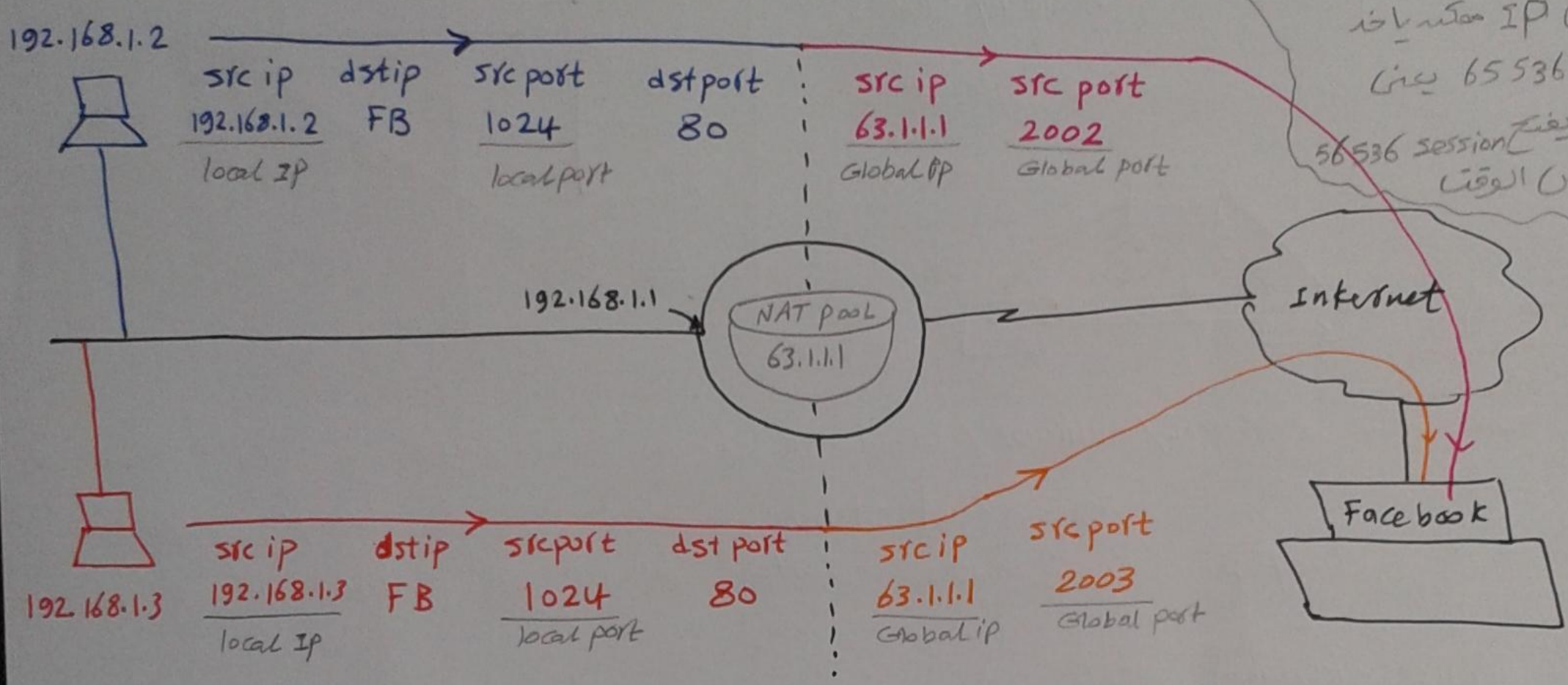
used for users many users ⟶ less public

---

[3] Dynamic NAT with overload

ex: PAT ≡ port address Translation





IP : port

socket no

Local IP:port	Global IP:port
192.168.1.2 : 1024	63.1.1.1 : 2002
192.168.1.3 : 1024	63.1.1.1 : 2003

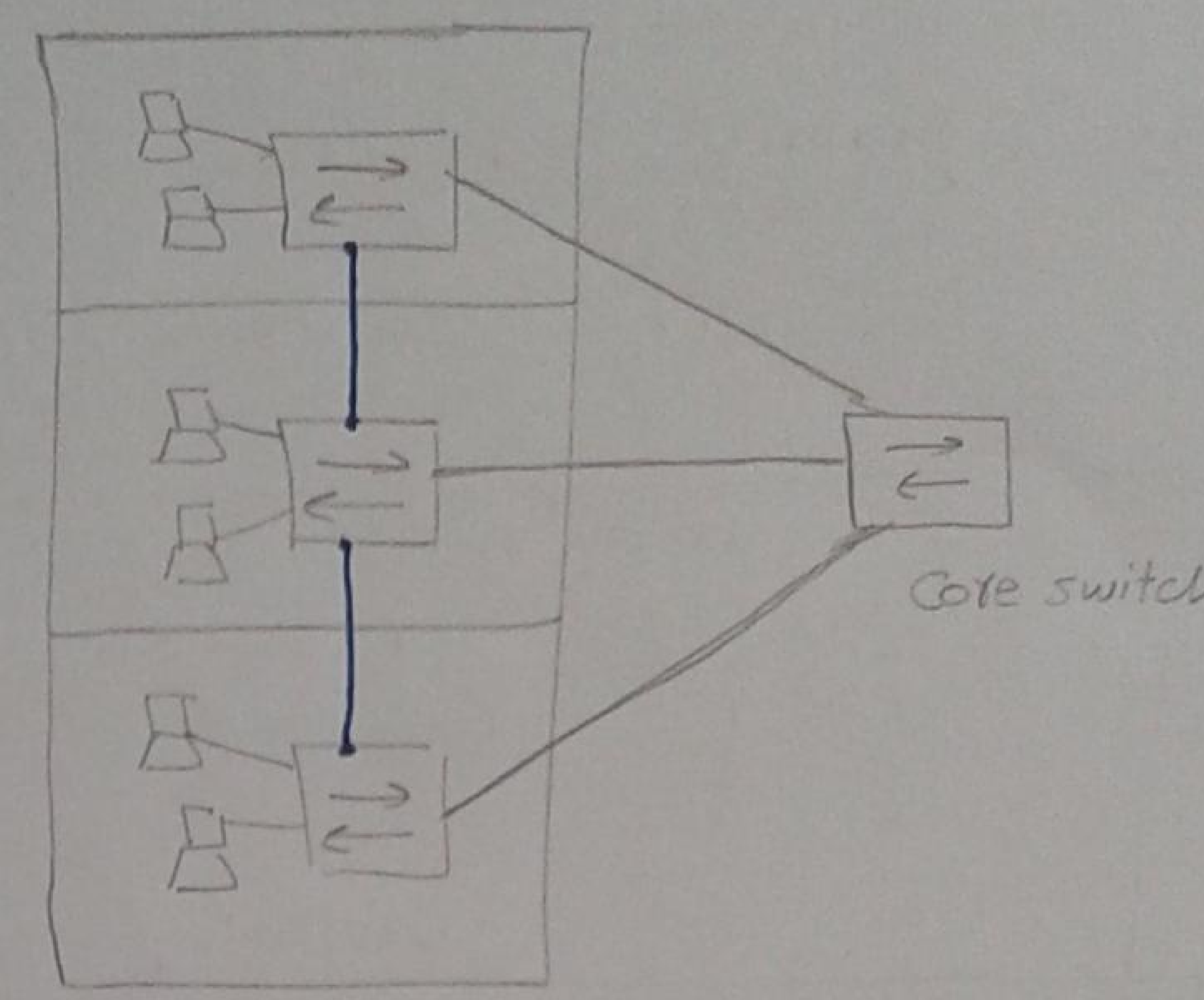
one public IP ممكن يستخدمه PC اكتر من نكرج التحفيش ، هنا

Switching

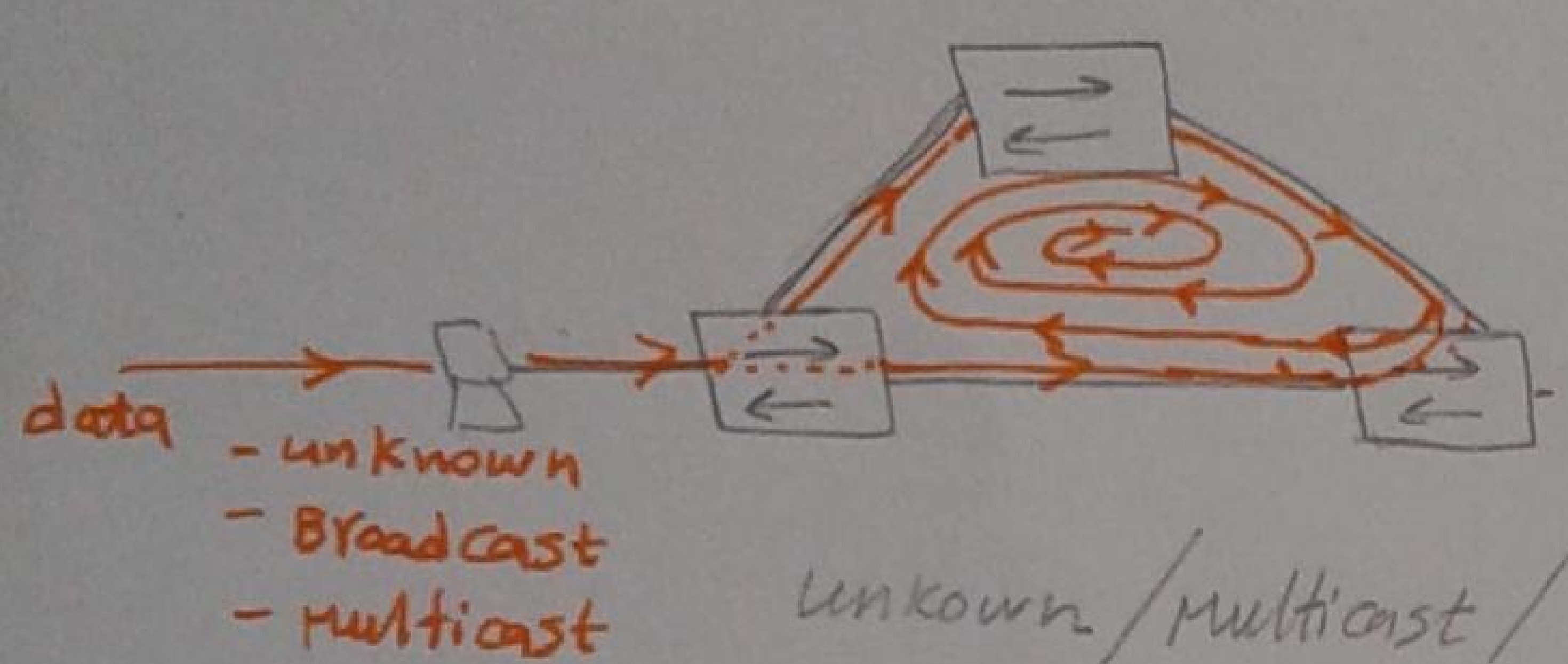
مبدئياً انا هفترض ان كل شغلي LAN

تحليل المشكلة

* عشان ازيد الـ redundancy بتاع الشبكة [لأن لو cable اتقطع هتكون النتيجة ان كل الاجهزة اللي وراه هتفصل] انا محتاج اضع Stand by cables [اللون الازرق]

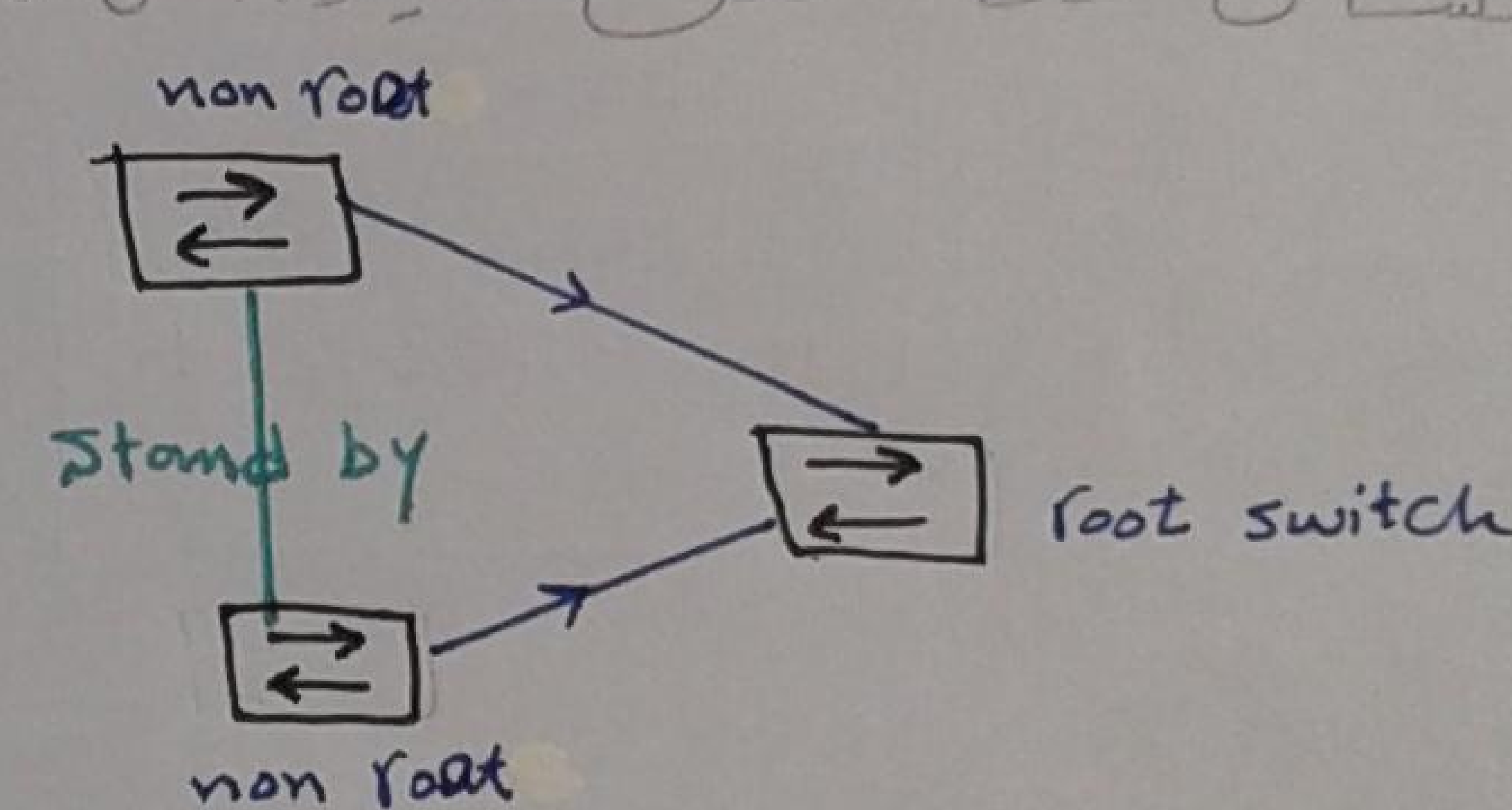


* للتبسيط بين ٣ سويتشات فقط



* لو في جهاز معين بيرسل Data نوعها Unkown/Multicast/Broadcast هيحصل loops كتير وهيسبب Broadcast storm
* لو عدد الـ Cables ≥ عدد الـ switchs ⟸ هيكون loops

عشان كده الحل هيكون في استخدام SPA [Spanning Tree algorithm]



* STP [Spanning Tree protocol] IEEE 802.1d

هنا الـ algorithm دة هيخلي طريقه pest والتاني Backup
ولو وقع الـ pest هيشغل الـ Backup

[I] at start up

(1) BPDU Flooding :- (Hello Flooding)

* each switch will form a Frame describing itself called BPDU [Bridge protocol Data unit] or you can say [Bridge Frame] and send it out out of all interfaces every 2 sec

في الاول كل الـ switchs هتبعت BPDU لحد ما ينتخبوا رئيس

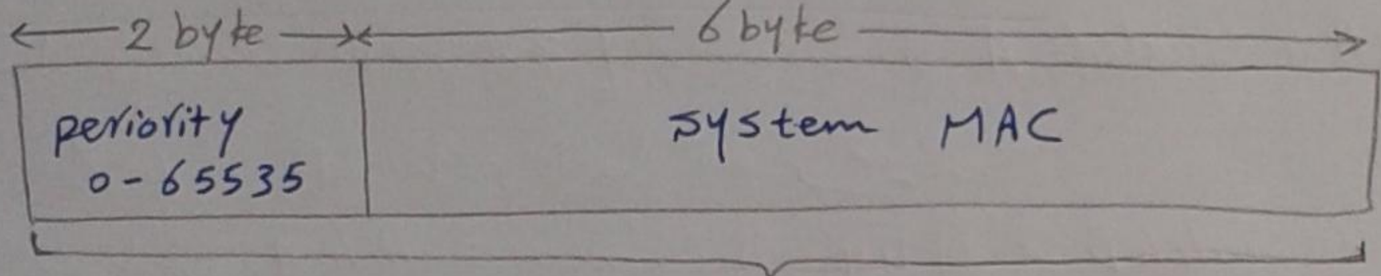
BPDU

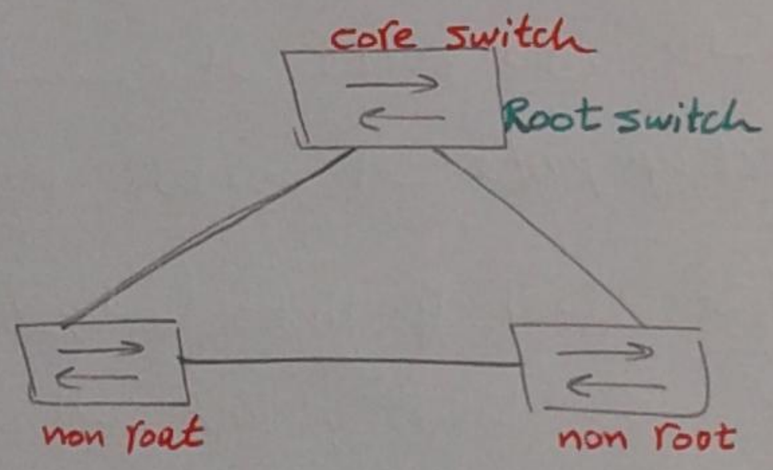
port ID	accumulated path cost	switch ID

② Electing root switch انتخاب الريس

انتخاب الريس بيكون على اساس اختيار افضل طريقه و الباقى يبقى Backup يعنى مش محتاجين خبرة زى ما كانه فى ال DR [Designater router]

* root switch is switch having least switch ID (MAC address or serial no)
  - بنستخدم ال serial no عشانه يقدروا يتواصلوا فى ال protocol دة فقط
  - * الاختيار بيكون على اساس الاقل periority
* periority is 2byte (16 bit) eig [0-65535]
* The default periority is 32,768
* to change periority by this order (config)# spanning-Tree VLAN periority #
* I set the lowest no of periority to the core switch





assume periority of A<B<C

note/ only root switch will send BPDU every 2 sec

---

③ Electing root port (RP)

Each non Root switch will choose the best port to reach root switch

RP is :-

(a) the port having least accumulated path cost Based on BW

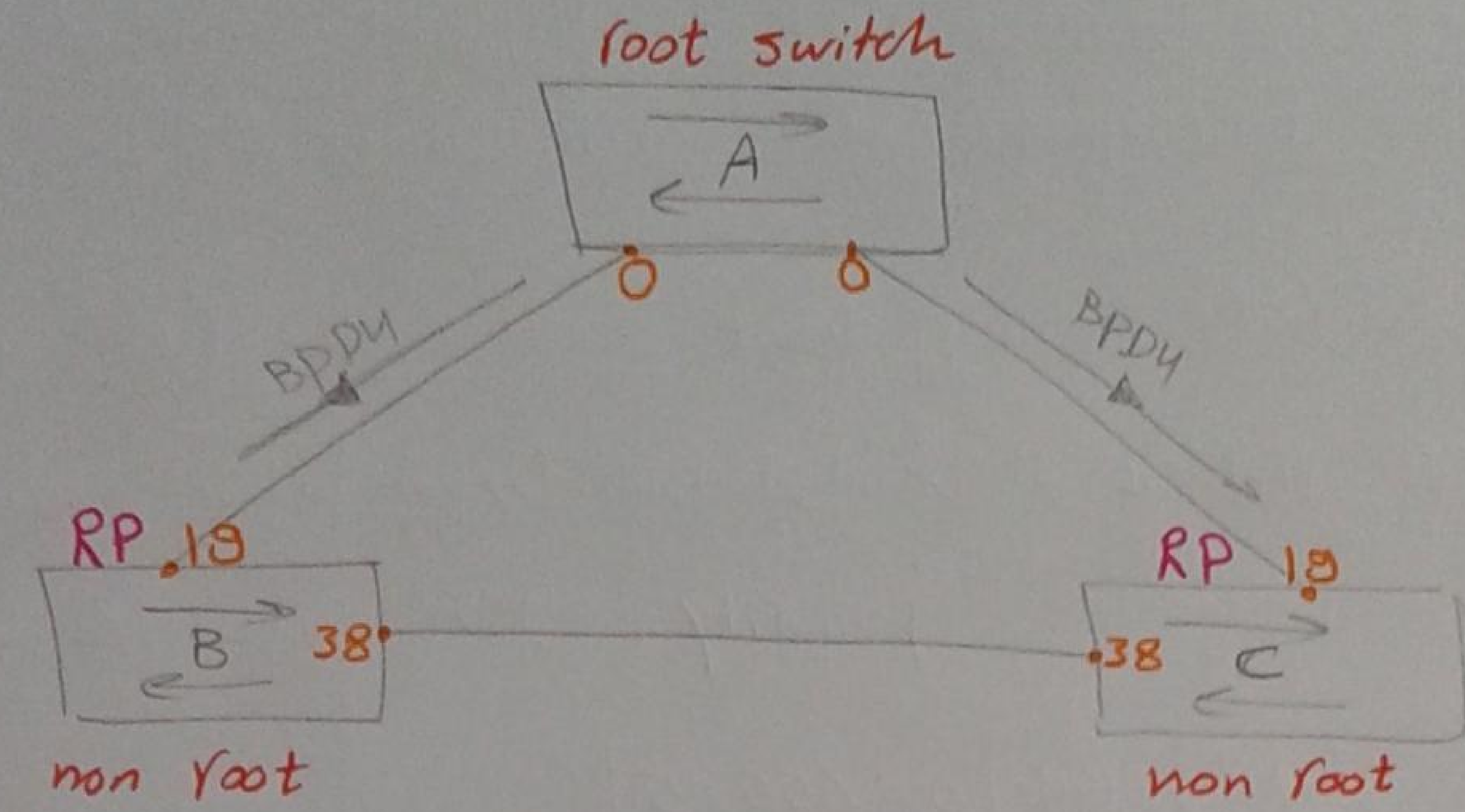
(b) port connected to least neighbor switch ID

(c) port connected to least neighbor port ID

اقل port ال

BW	Cost
10 Mbps	100
100 Mbps	19
1G bps	4
10 G bps	2

* we assume that all links are Fast Ethernet [100 Mbps] ∴ the cost = 19

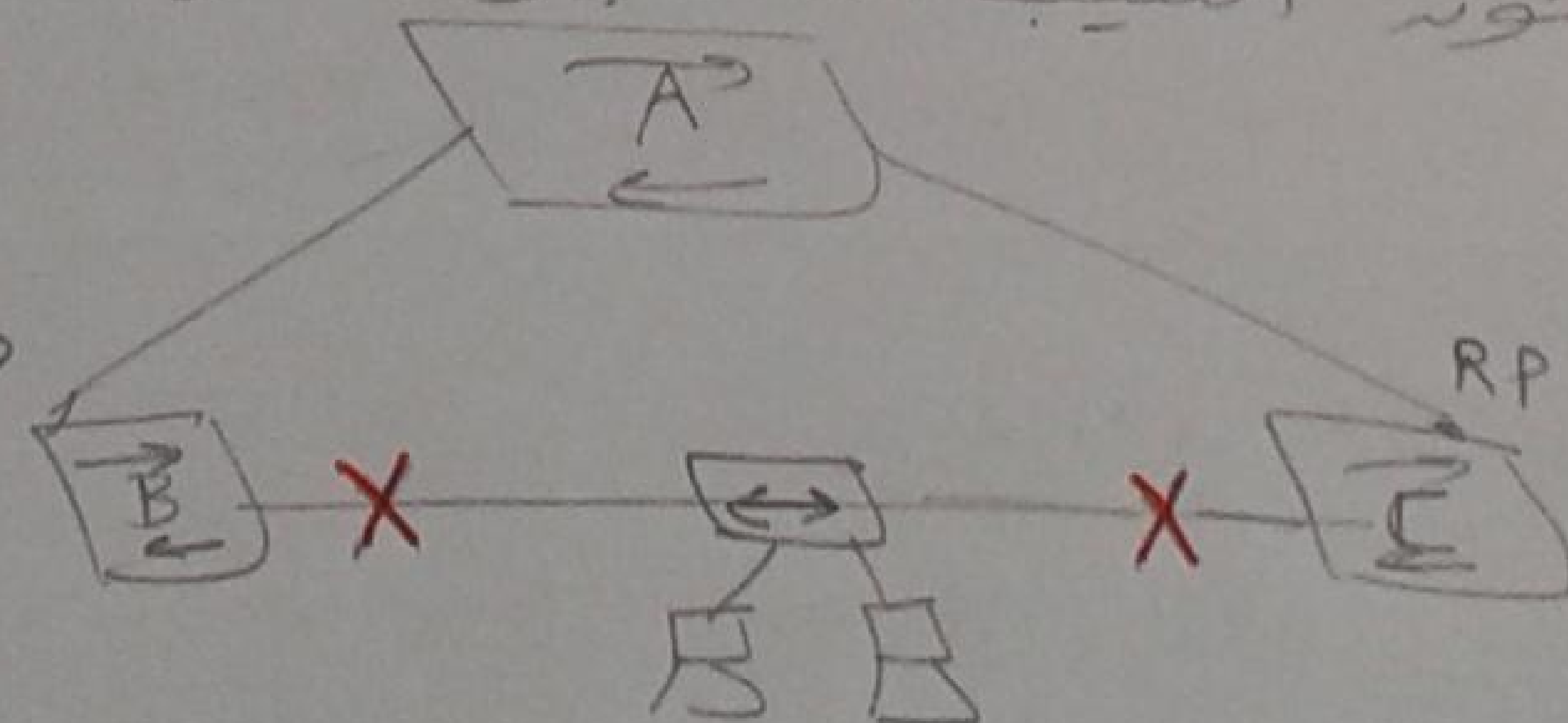


* switch A هيبعت BPDU] بـ cost تساوى 0] لـ switch C و switch C هيشوف
السرعه وهيلاقيها 100 Mbps و switch C هيضيف الـ cost المناظر للسرعه 100 Mbps اللى
هو 19 للـ BPDU Frame وهيبعته لـ switch B و بنفس الطريقه switch B
هيضيف 19 [هيبقى الناتج 38] وهيبعته لـ switch A و switch A لما ترجعله
الـ BPDU هيلاقى الـ ID بتاعه عليها فهيرميها

* من طريقه تانى switch A هيبعت الـ BPDU لـ switch B و هيحصل نفس الحكايه

* كل non root switch هيختار The best port من الـ ports بتاعه اللى بتوصله
للـ root switch وهيسمى الـ ports دى بالـ Root ports [RP]
وهيسمى الـ ports التانيه بالـ Back up ports

* لاحظ انه مش بيجعلها Back up links عشان ما تقابلش اشكاليه ان فى
اجهزة متوصله فى الـ Back up link ده زى الحاله دى لو احنا فصلنا
الـ 2 ports ⇐ هتكون النتيجه ان الاجهزة المتوصله بالـ link ده هتفصل



عشان كده هروح لخطوة (4)
وهو انه بدل ما اجعل الطرفين بتاع الـ link يكونوا Blocked ← هجعل
واحد بس Blocked

4 Electing Disignated port [DP]

* it is the best port on each segment [link] that can reach the root switch

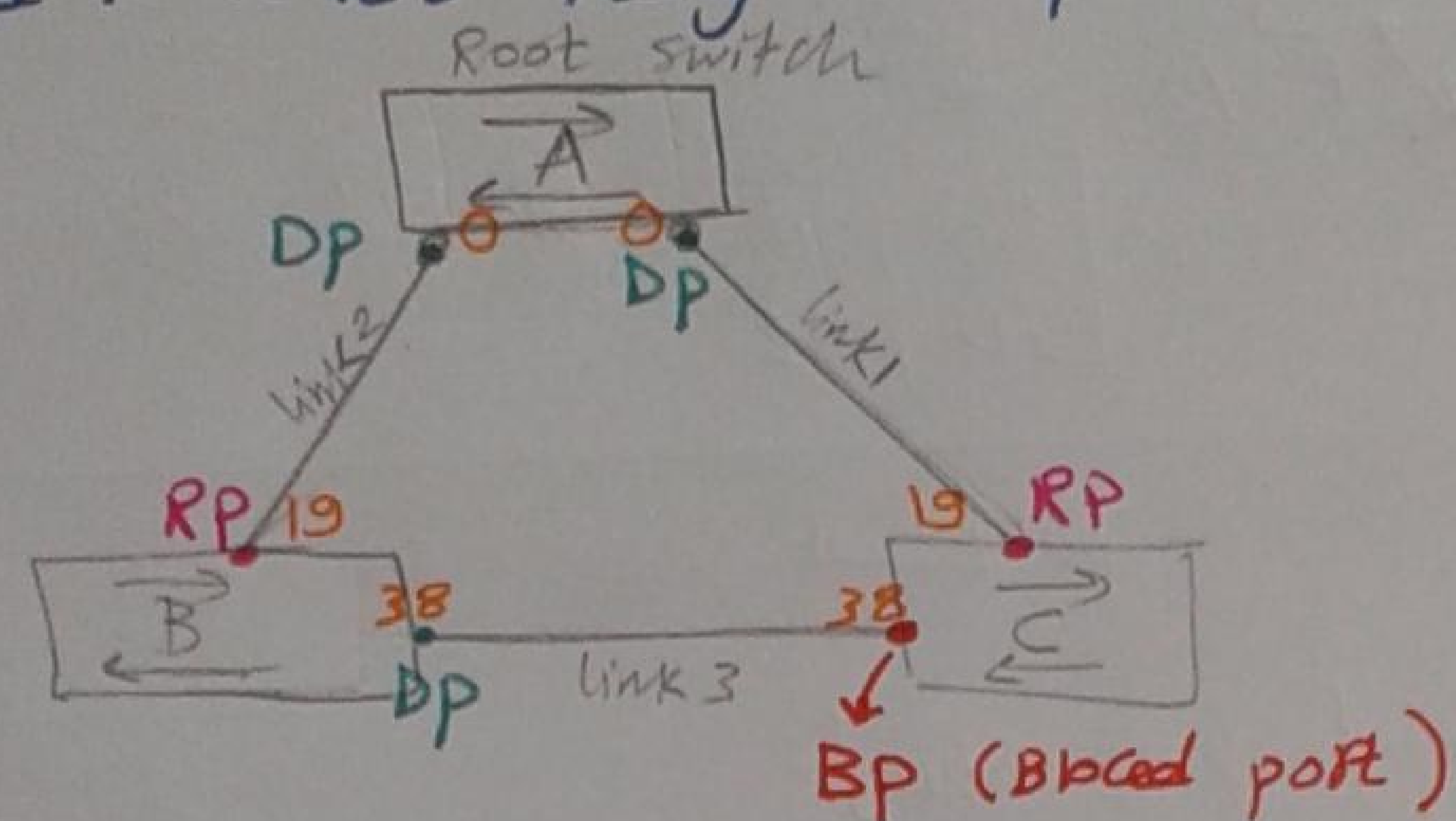
احسن port على ال link

DP is

ⓐ port having least accumolated path cost Based on BW

ⓑ port connected to least neighbor switch ID

ⓒ port connected to least neighbor port ID



* في link 1 & 2 هيشوف ال port اللي عليه اقل cost هيخترها ك (DP)
* في link3 هيلاقي ان ال 2 ports بتاعة ال link دة ليهم نفس ال cost (38) فهيشوف نقطة ⓑ فهيلاقي ال switchB له ID اقل وبالتالي هيختار ال port بتاعه switch B ويسميه ال (DP) وبالتالي مش هيبقى الا ال port اللي ناحيه switch C ودي بقى هيخليها ال BP [Blocked port]

5 Blocked port (BP)

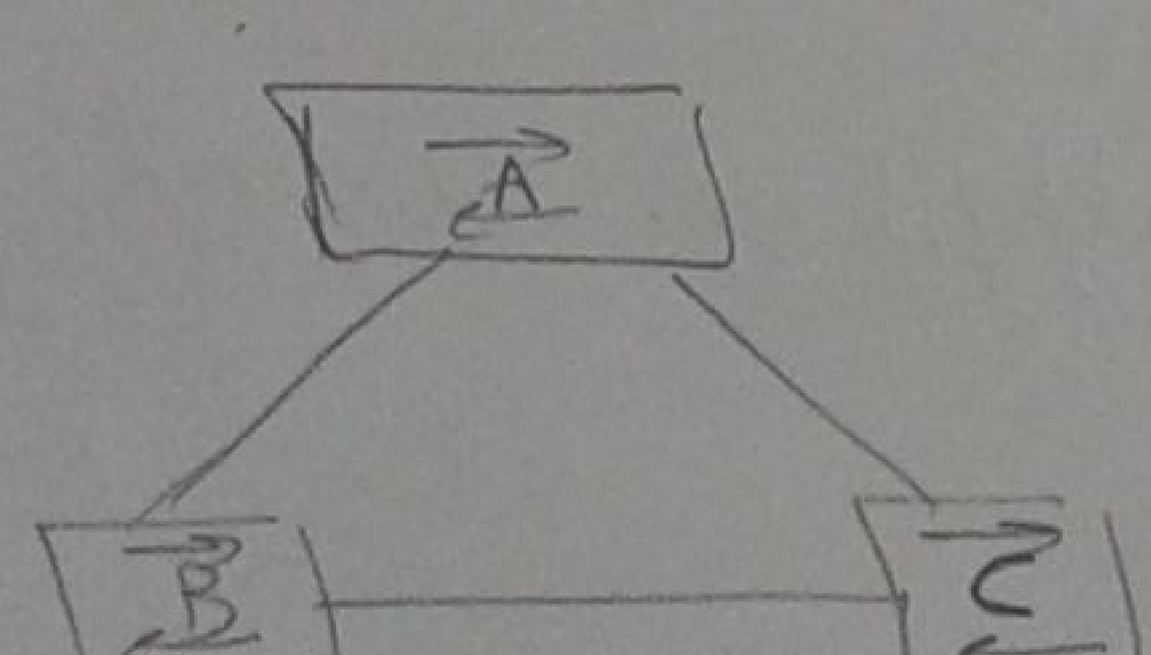
* ports that are neither RP nor DP

ال port دي بتبقى مقفوله logical بمعنى انه لو جه عليها Data ⇐ هتوقفها يعني هتعملها drop

---

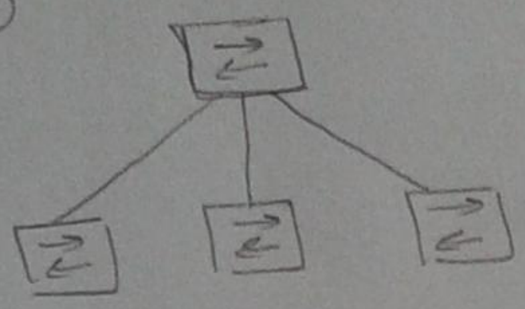
∴ no of BPs = no of links − no of switchs + 1

(ex.1)



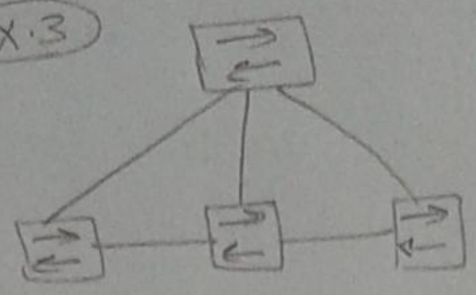
no of BPs = 3 − 3 + 1 = 1

ex.2



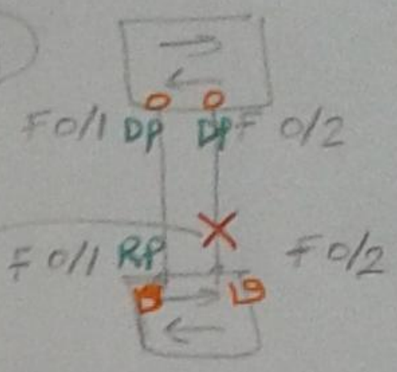
BPs = 3-4+1 = 0

ex.3



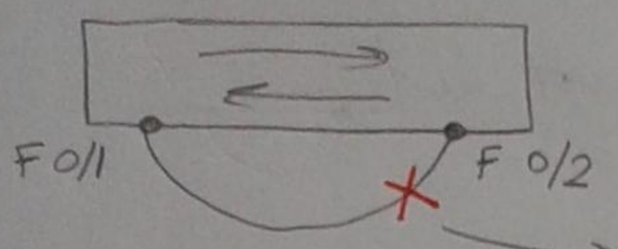
BPs = 5-4+1 = 2

ex.4



BPs = 2-2+1 = 1

ex.5



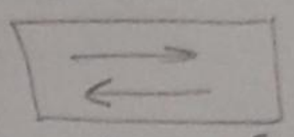
[this port is blocked because it has least ID port]

---

port منشوف منا من وجهه نظر الـ

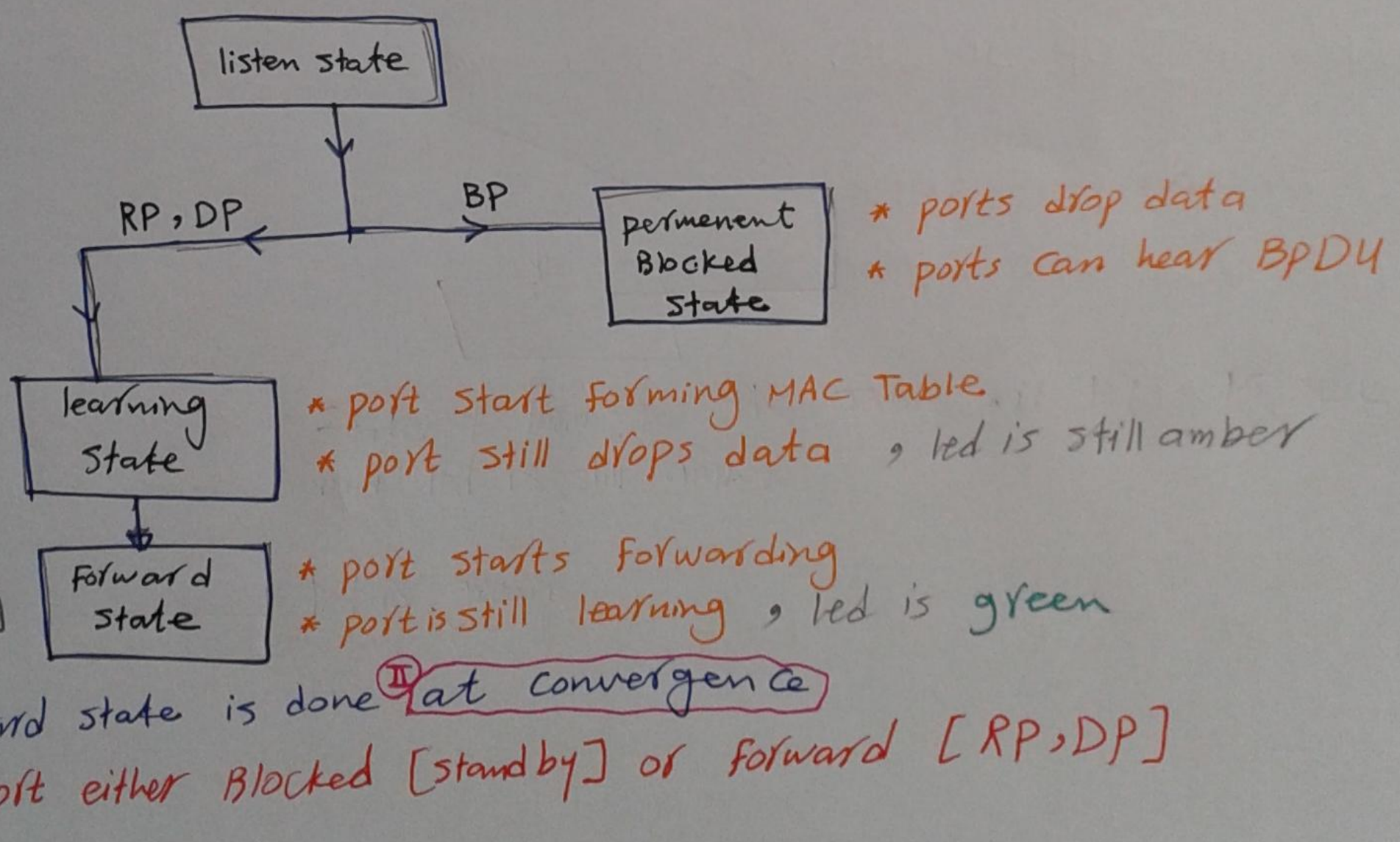
led

Black — Disable state [e.g no cable]



yellow — Temporary Blocked state ← during port load config. < 2sec

Amber — listen state [15 sec]
* ports start elections [RP > DP > BP]
* ports drop data

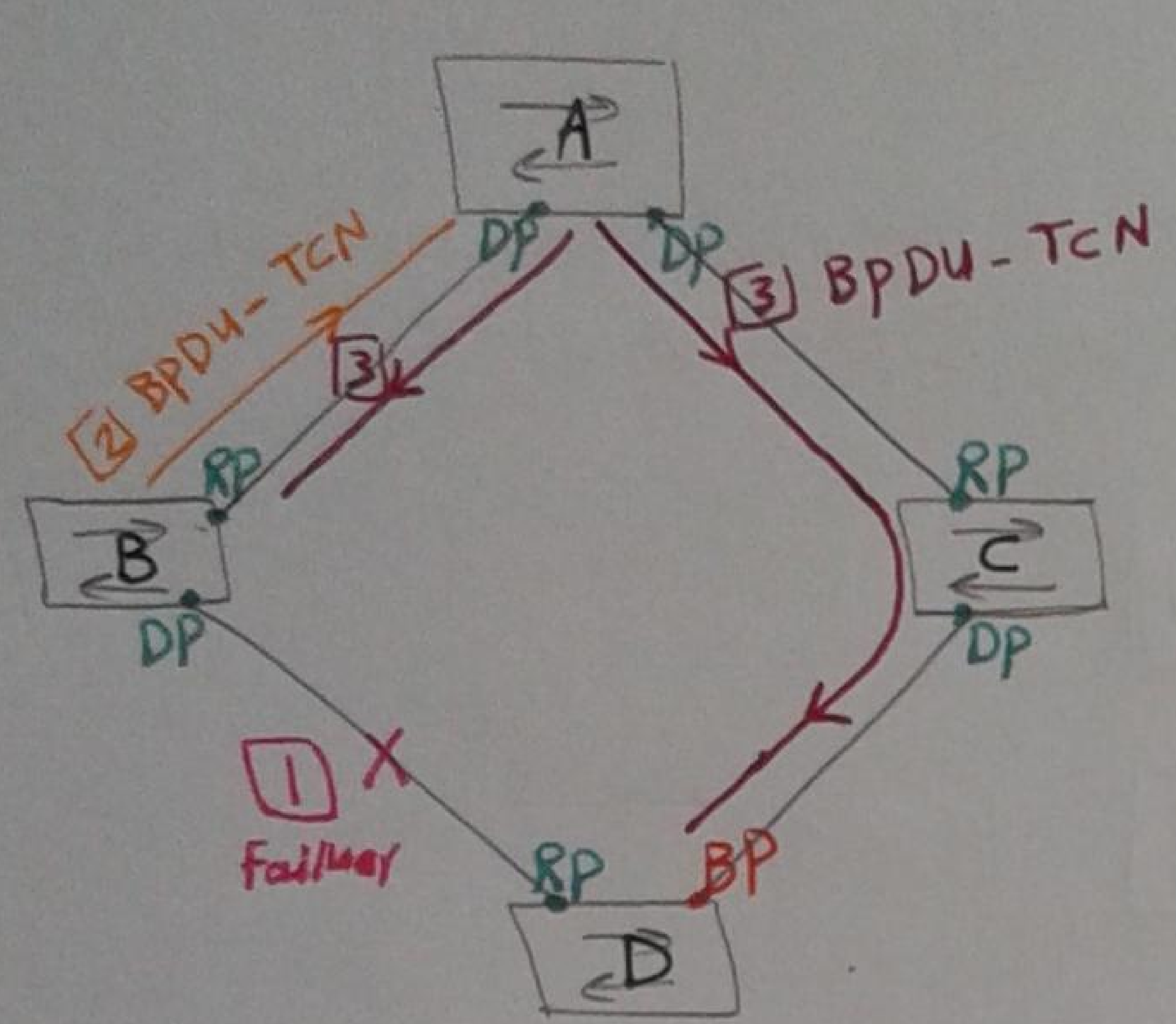


Forward state is done at convergence

∴ port either Blocked [standby] or forward [RP, DP]

III at change

1 direct change

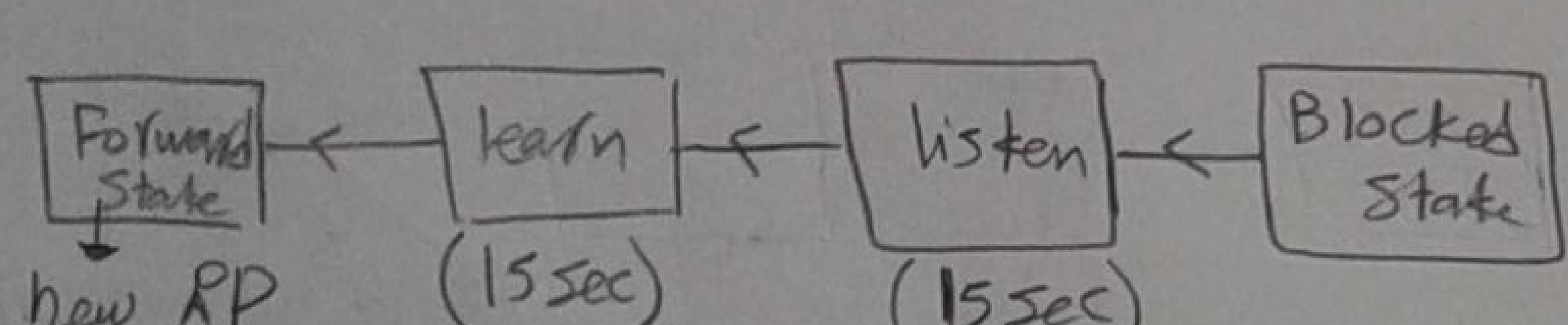


1. Failure is exists
2. switch that feels the change will send triggered BPDU-TCN to root switch
   (TCN: topology change notification)

* في حالتنا switch B هو اللي هيبعت BPDU-TCN

3. the root switch [switch A] will send BPDU-TCN to all ports by Flooding

وهنا كل ال BPs هتعيد حساباتها من اول وجديد



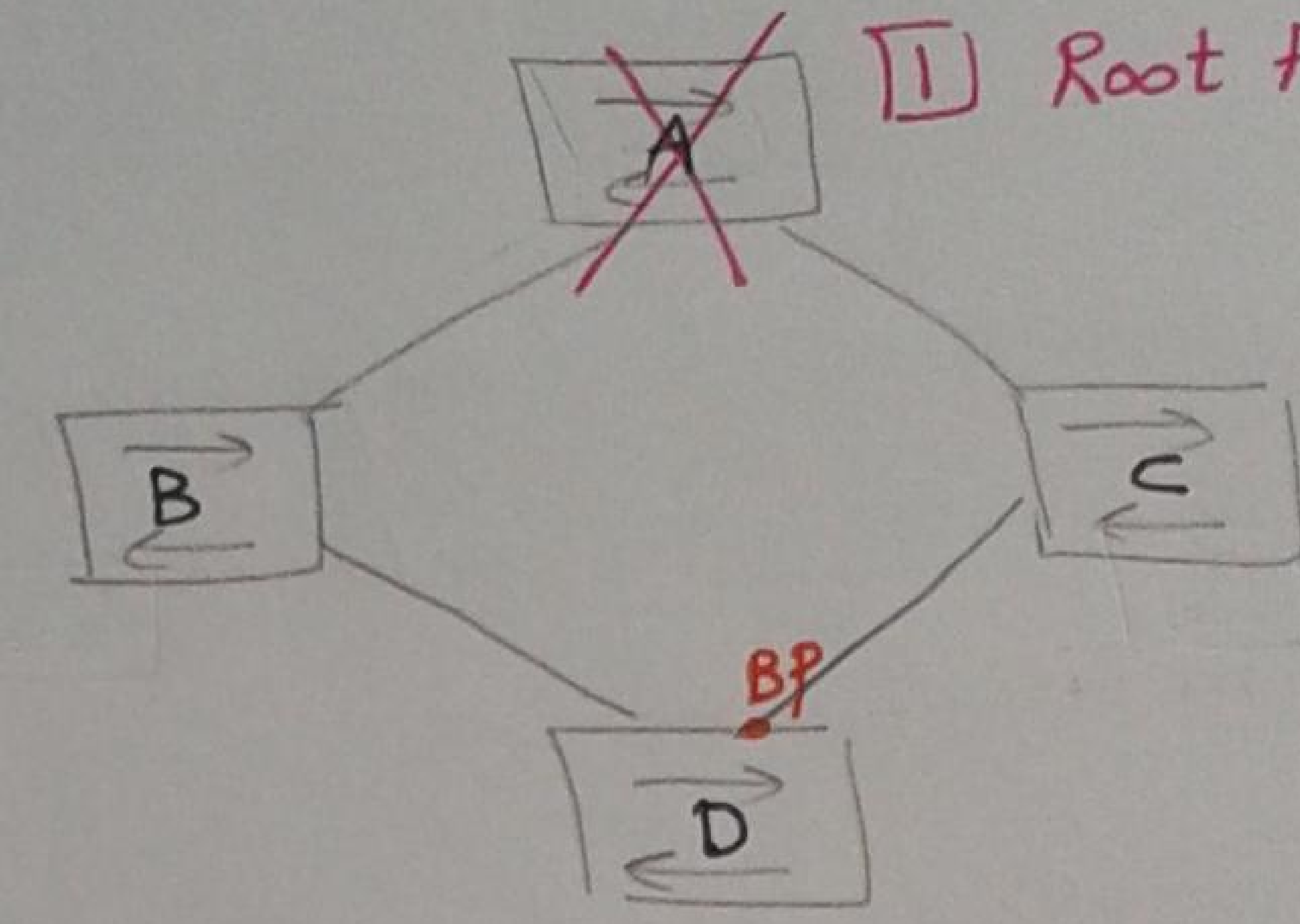
العمليه دي هتاخد وقت أكثر من 30 sec

عشان يوصل لل Convergence time

Conv. time = 30 sec

2 Indirect change

1 Root failed



في الحاله دي ال Blocked port قبل ما هتبدأ

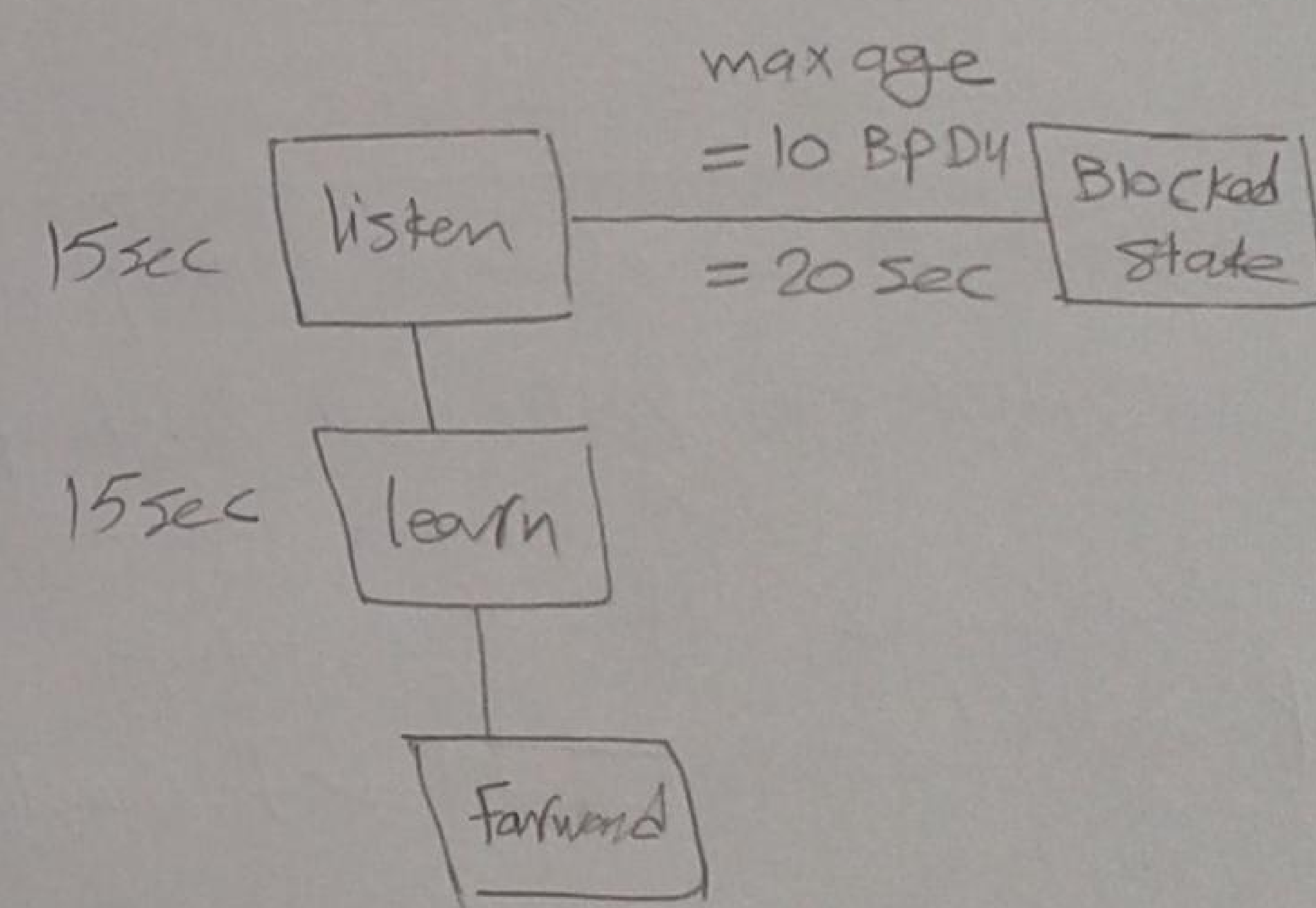
تعيد حساباتها هتثبت (BPDU msg) زي ال Hello

١٠ مرات بين الواحدة والتانية ثانيتين

∴ ال switches هتنتظر ١٠ * 2 = 20 sec

ولو ال Root switch لم يرد ، كل

ال switchs هتعمل انتخابات من الاول



Convergence time = 50 sec

∴ the conv. time between 30 & 50 sec ⟹ that is no accepted , so there will be RSTP

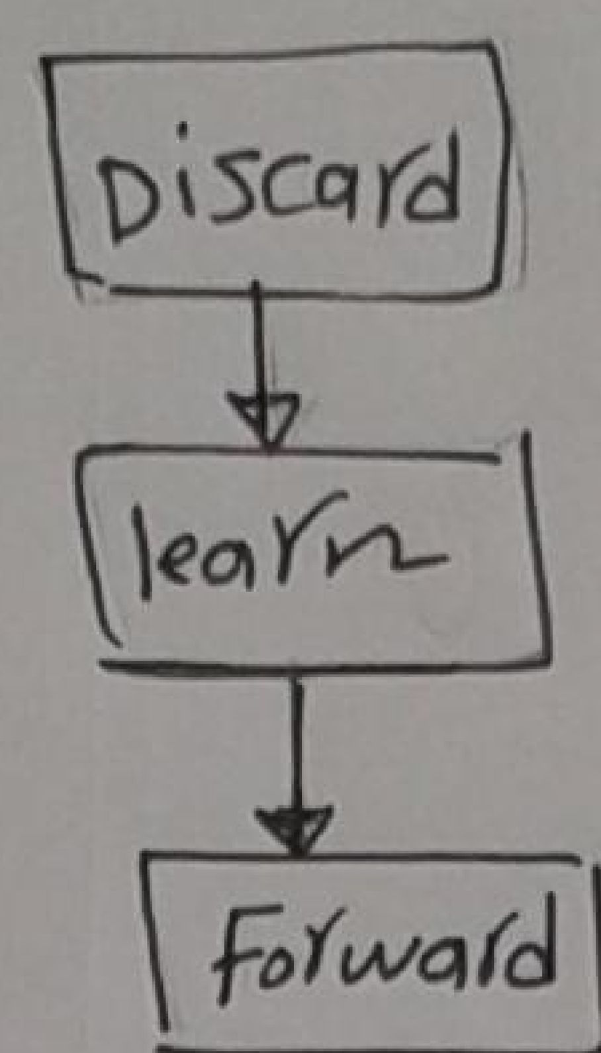
* RSTP [Rapid STP]   IEEE 802.1 W

it was [STP + cisco Enhancement = ESTP]   كان في الاصل بتاع cisco
لكن ال IEEE اخدته كـ standard

First Enhancement / they grouped disable & blocked & listen states in to one state called Discard state

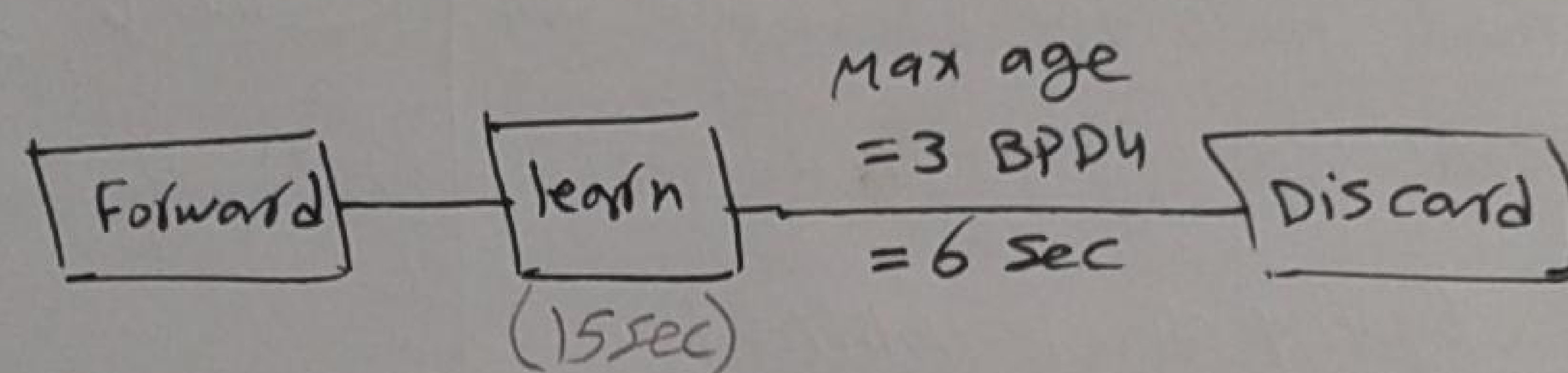
① in direct change

بكده انا حسنت من 30sec الى 15sec



∴ Conv. time = 15 Sec

② in Indirect change



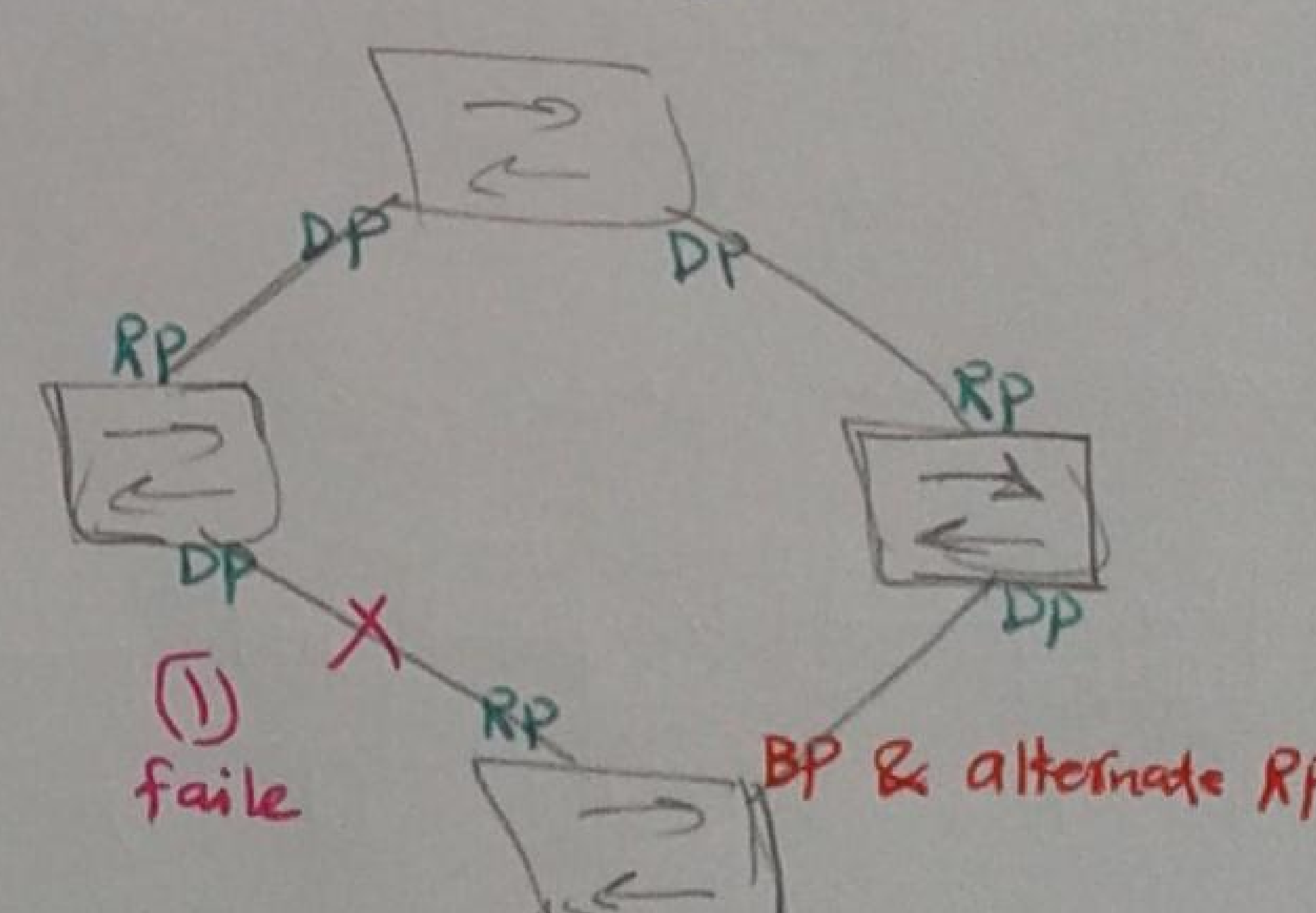
Conv. time = 21 Sec

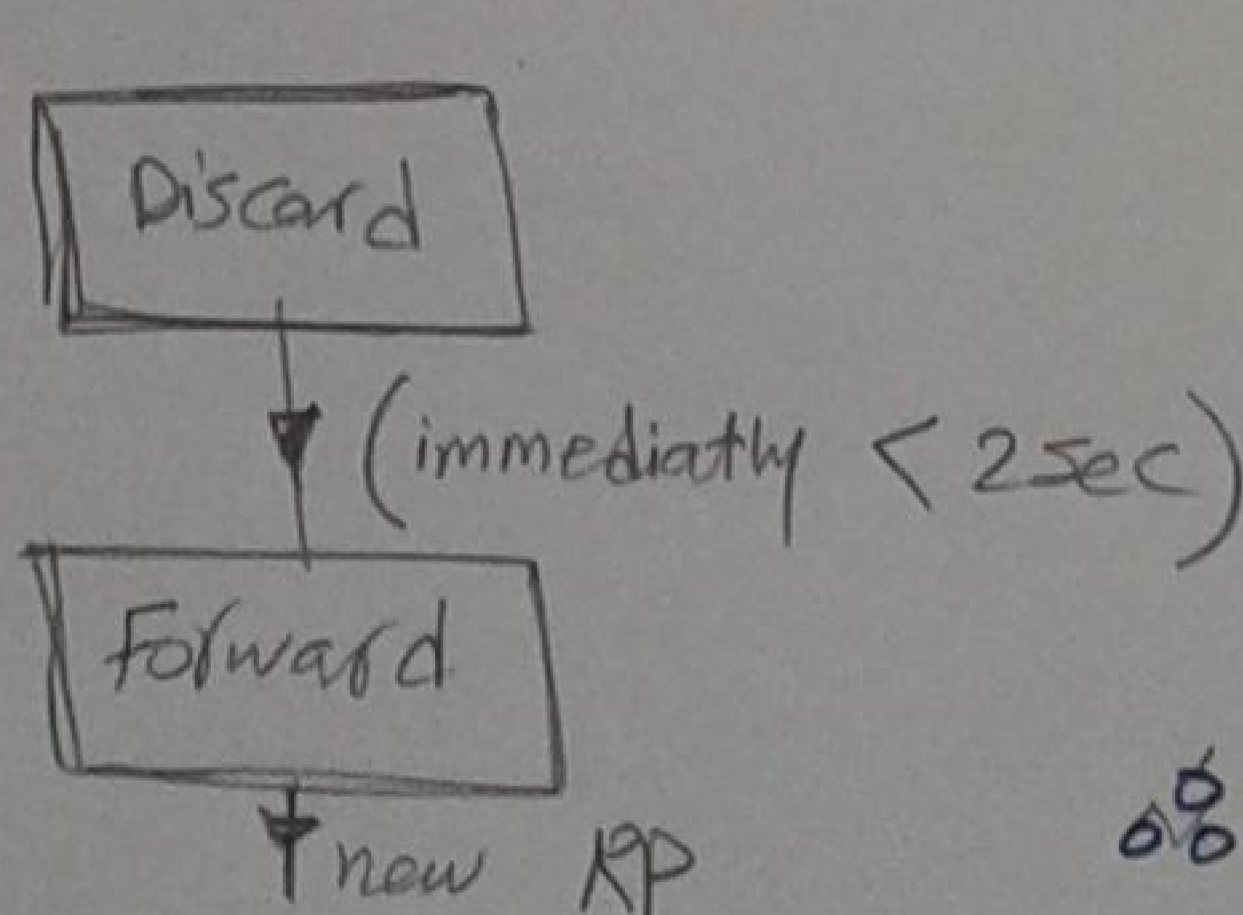
---

second Enhancement / they introduce extra elections [new port rules]
→ alternate port and Backup port For each [RP & DP]

① Direct change

بمجرد ما يحصل Faluire ، ال BP تروح محوله
نفسها Immediatly [في اقل من 2sec] الى RP





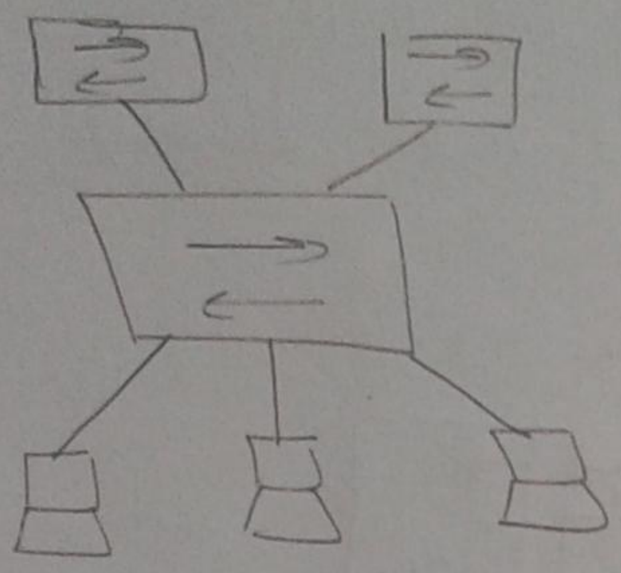
∴ conv. time < 2 sec

---

② indirect change

في الحالة دي لازم يتم انتخابات من اول وجديد عشان كدة كان الحل انهم
يهتموا اوي بال Root switch في انه متفصلش منه power supply معها كان

third Enhancement / they introduce a concept called port fast / port fast / port that jump to forward state immediatly , it should be used with ports connected to PCs (DTEs)



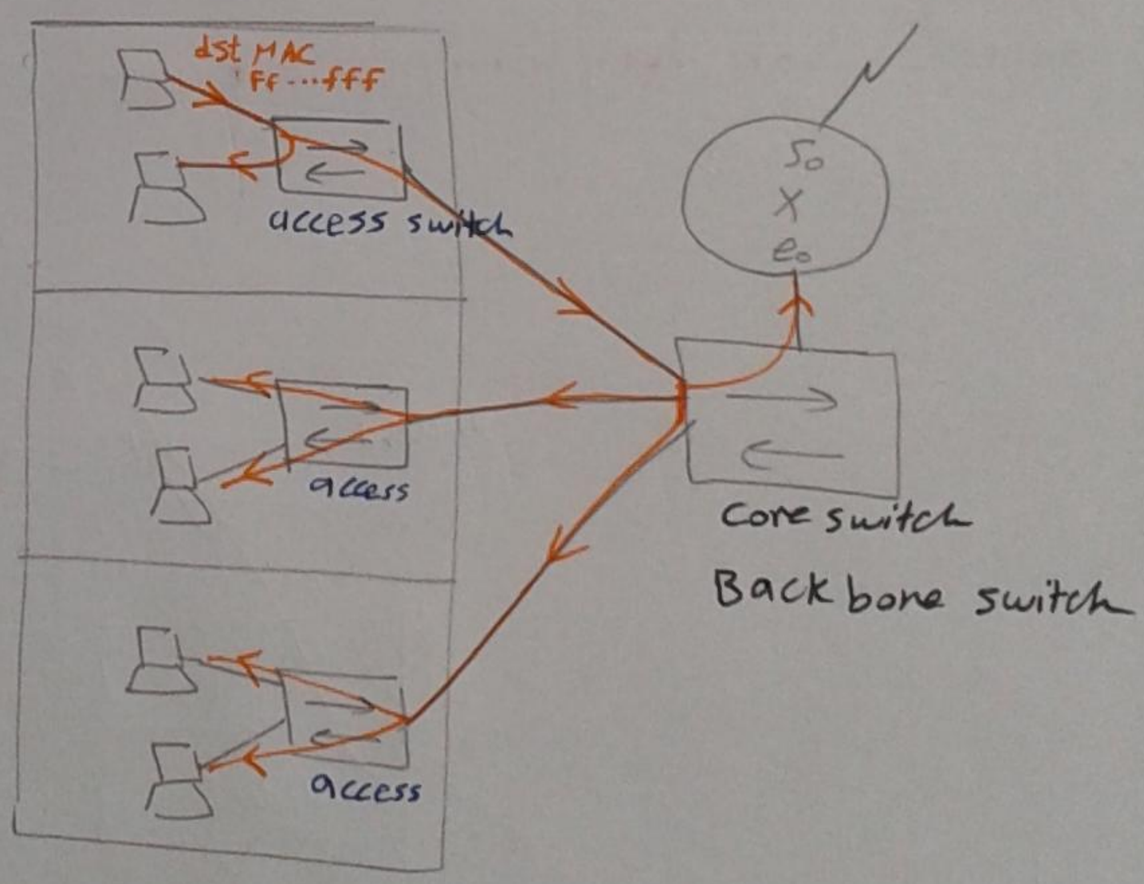
الخاصيه دى عشان ال PC لو عمل Restart هيستنظرش 50 sec عشان يا يتوصل بال Network و اول ما ال PC ← Restart ← ال port اللى متوصل بيه هش هيحس بيه ويوصله على طول بال Network

(config-If) # spanning-Tree port Fast

The main problem here is Flooding

food occures when → Broadcast
→ Mullicast
→ unknown unicast

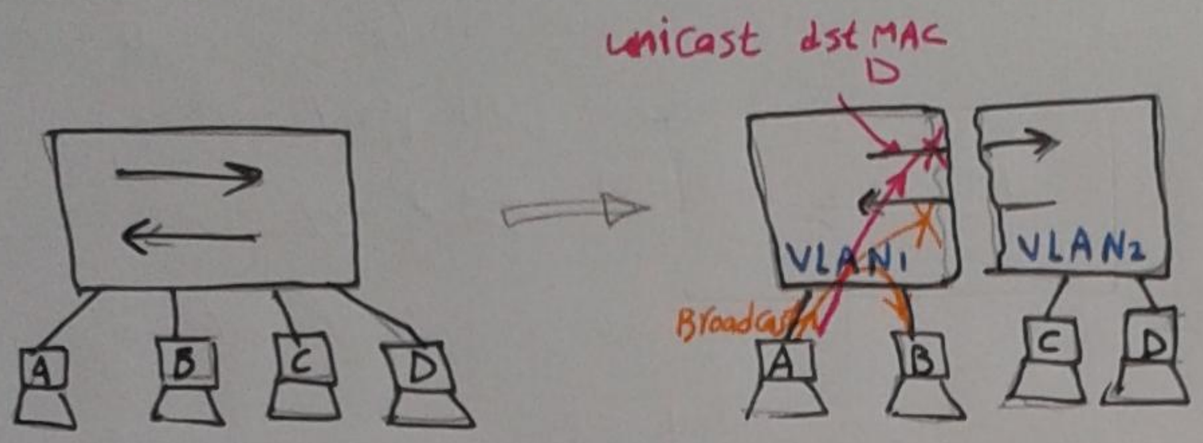
عليه ال Flood بتخنق الشبكه جدا



The solution is using VLAN [vertual LAN]

VLAN : vertual LAN [it works as softwere Isolation]

* we devide one physical switch to more than one vertual switch
* you can make every port on a switch as VLAN
* max. number of VLANs per switch = 4096 (12 bit)
* the use of VLANs is to decrease flooding



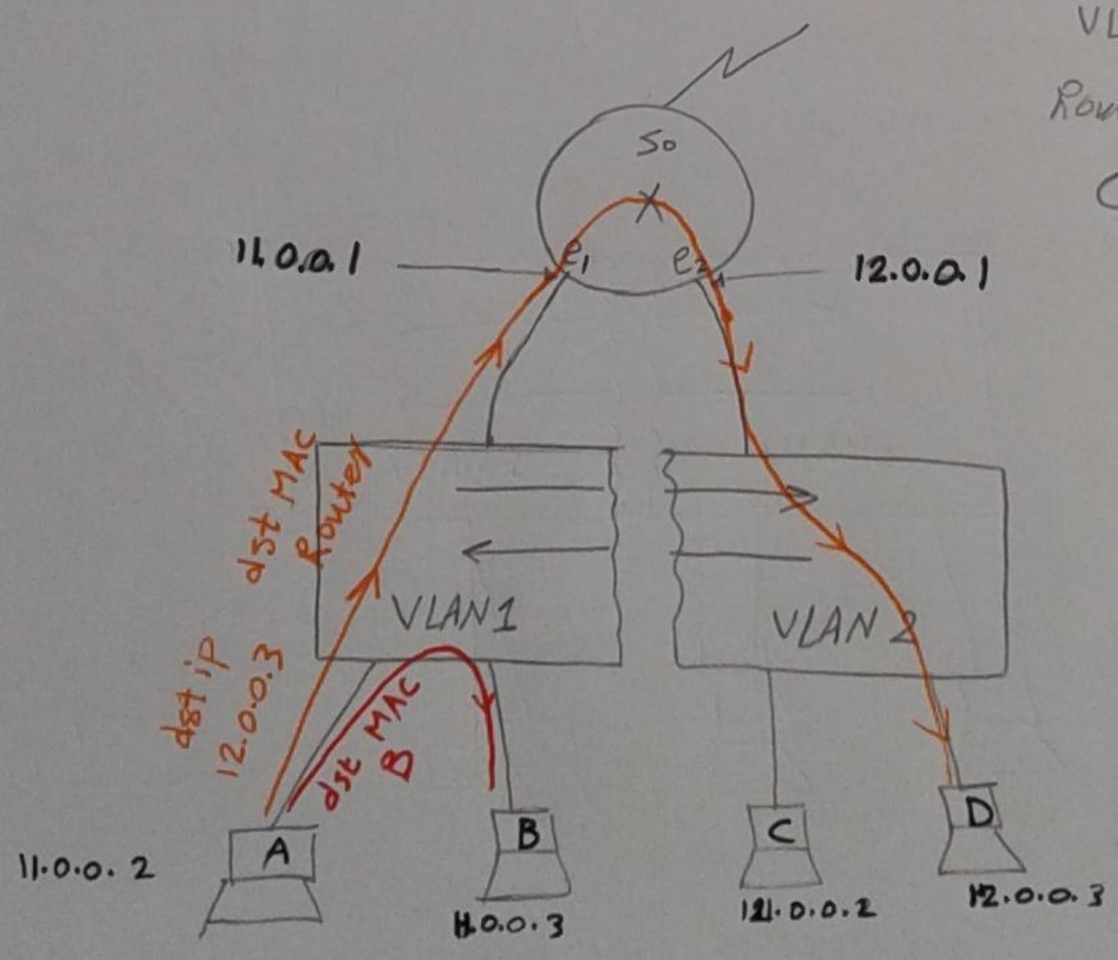
مفيش Broadcast هيمر من VLAN1 الى VLAN2 ودة كويس
لكنه المشكله انه هيوقع الداتا
اللى رايحه unicast من
VLAN الى VLAN2 ودة مشكله عشانه كنا هنفكر فى استخدام Router

→ each VLAN is a broadcast domain

* Inter VLAN Routing العلن فى

(1) Traditional solution (5% of usage)

* هنا بنستخدم Router وبنعتمد على مزاياه انه لا يبعت broadcast ولا بيعمل Flooding
* ملحوظه / اجعل لكل VLAN ← subnet



* الشكله هنا انى هحتاج لكل VLAN كابل + Interface خاصه على الـ Router
والـ Interface دة بيبقى غالى اوى

* ملحوظه/ الـ PC مش بيفهم يعنى ايه VLAN لكنه بيفهم Subnets

[2] Router on a stick (75% of usage)

هنا مستخدم port - واحدة بين ال switch واقرب اوصل لأي VLAN عن طريق

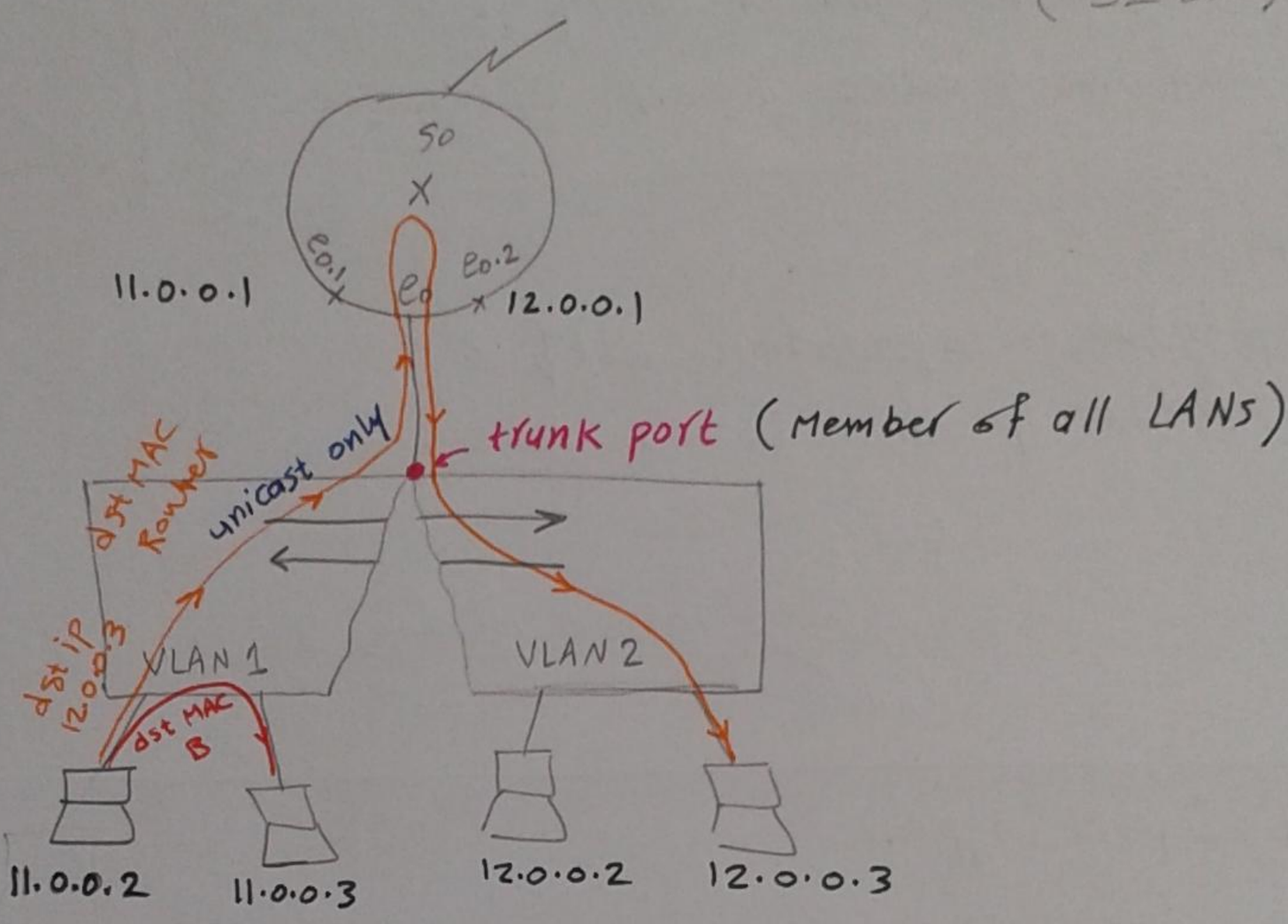
ال port دي واوصل ال port دي ← Interface واحدة بين ال Router

[trunk port]

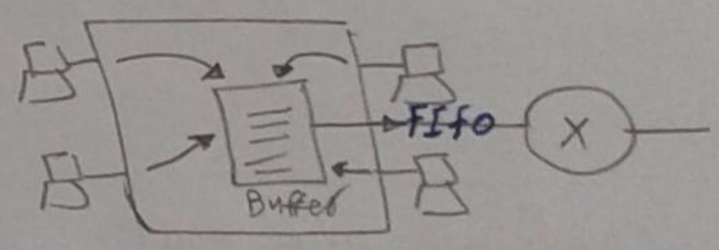
* اقسم ال Interface اللي جاي ال Router الى vertual subinterfaces

* اقدر اقسم ال Interface الواحدة جاي ال Router الى 4,xxx,xxx,xxx vertual subinterfaces

(32 bit)



* the trunk port must have very High B.W ⟹ مثلا كل ال PCs بتستخدم ال unicast



Disadvantage

1- congistion

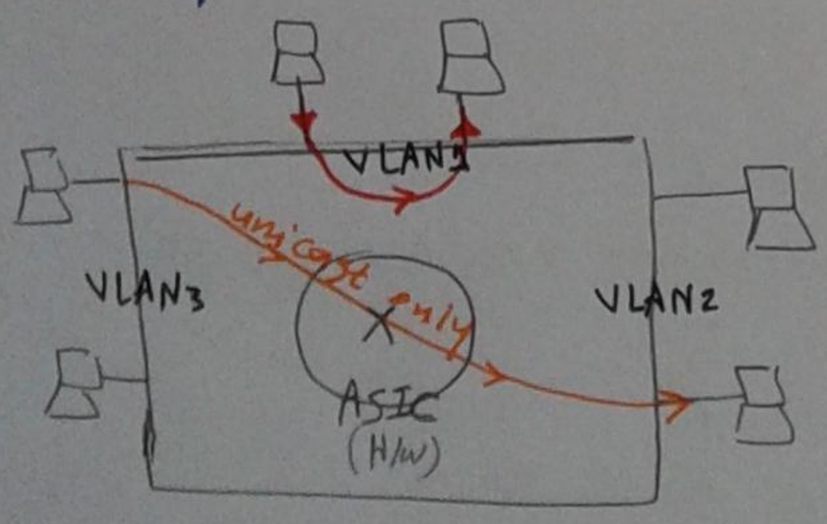
2- Single point of failure (i.e) If the trunk port is cut, the all Network will be fallen

3- S/W Based because of Router

---

[3] Multilayer switch (20% of usage)

→ layer 3 switch



* هو في الاساس switch مثلا كل ال ports base the same comm. Technology

* هو حل ال 2 مشاكل اللي فاتو لكن بيه very Expensive انه

* The configuration for [2] Router on a stick

General

```
(config) # int e0
(config-if) # no shut down
(config-If) # no ip address
```

For e0.1

```
(config) # int e0.1
(config-subif) # encapsulation dot1q 1   ← VLAN no
(config-subif) # ip address 11.0.0.1 255.255.255.0
```

For e0.2

```
(config) # int e0.2
(config-subif) # encapsulation dot1q 2
(config-subif) # ip address 12.0.0.1 255.255.255.0
```

e0.1
e0.2
e0.3
:
e0.N

← virtual interfaces عدد ال حسب على تكون تانى تقدر

---

* switch port types

[1] access port

* it is a port that is a member in only one VLAN
* it is a port that is connected from switch to PC

to configure one port	to configure range of ports
(config) # inerface F (0/3) ← Fast Ethernet, port no (config-If) # switchport Mode access	(config) # interface range f 0/3-15, 19 From 3. to 15 and 19 (config-If) switch port Mode access

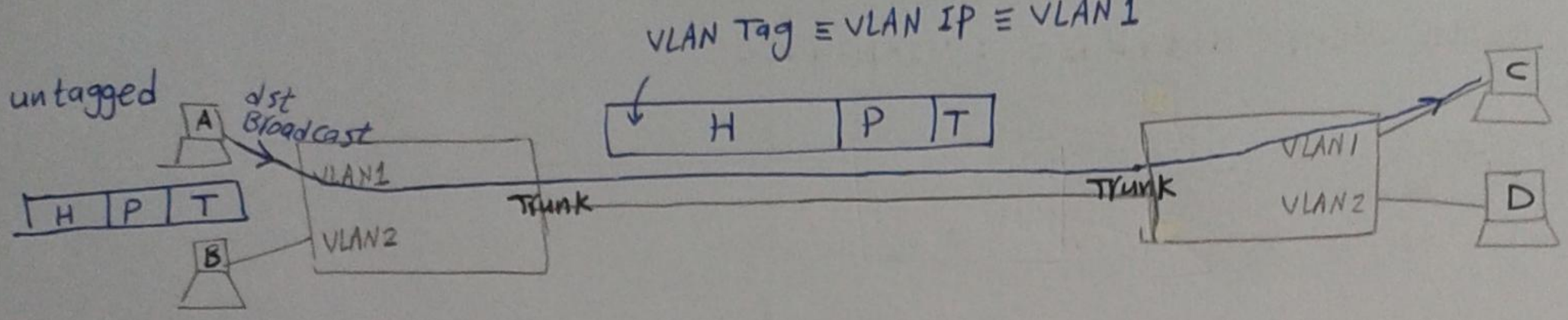
ملحوظه / لما تقول لل port انت access ← هيعتبر نفسه فى (Native LAN) default LAN
الى هو VLAN1 و تقدر تغيره بال Configuration

[2] Trunk port

* it is a port that is a member of all VLANS by default
* That port is a port connected from switch to a router or to another switch

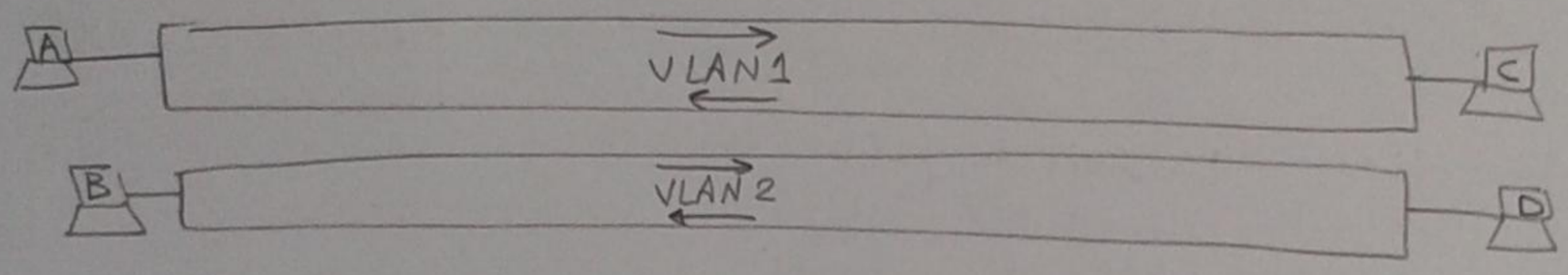
```
(config) # int f 0/24
(config-If) # switchport Mode trunk
```

Trunk of switch to switch



ال Trunk switch بيضيف ال Tag ال frame عشان يقدر يعمل Broadcast على نفس VLAN بس متوصله بـ switch مختلف وال Tag دة بيبقى فيه اسم ال VLAN ⇒ VLAN ID

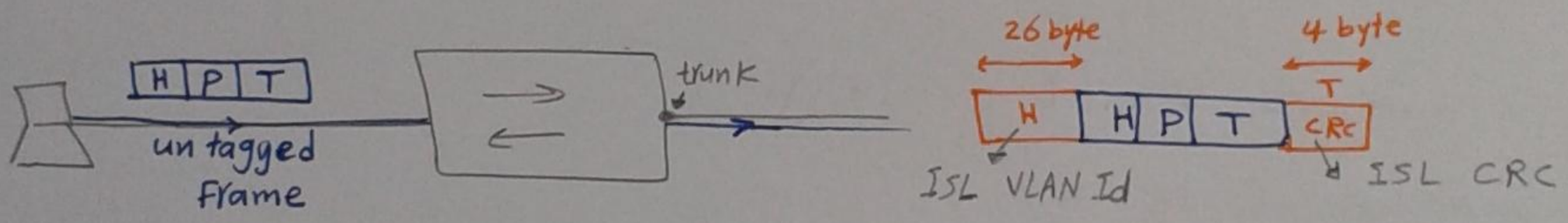
∞ VLAN can span multiple switches



---

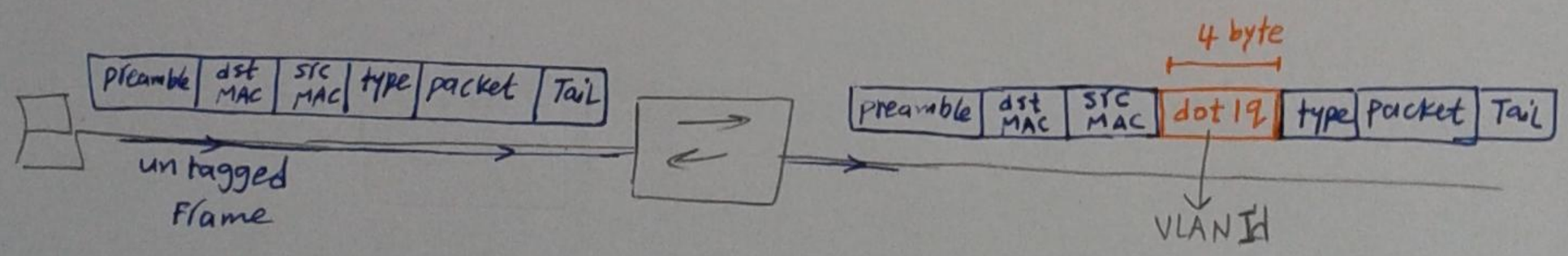
* Tagged types

[1] ISL [inter switch link] by Cisco



لكنه فشل لانك اضفت 30byte ⇐ كتير اوى

[2] IEEE 802.1q



VLAN configuration

[1] create VLAN database : VLAN.date

(config)# VLAN VLAN #

(config-VLAN)# Name VLAN name → option

to show VLANS → ✻ show VLAN

EX

(config)# VLAN 2
(config-VLAN)# name HR
(config)# VLAN 3
(config-VLAN)# sales
⋮

you can configure all data base on one switch and spann them

number #	Name
VLAN 1	default
VLAN 2	HR
VLAN 3	sales
⋮	

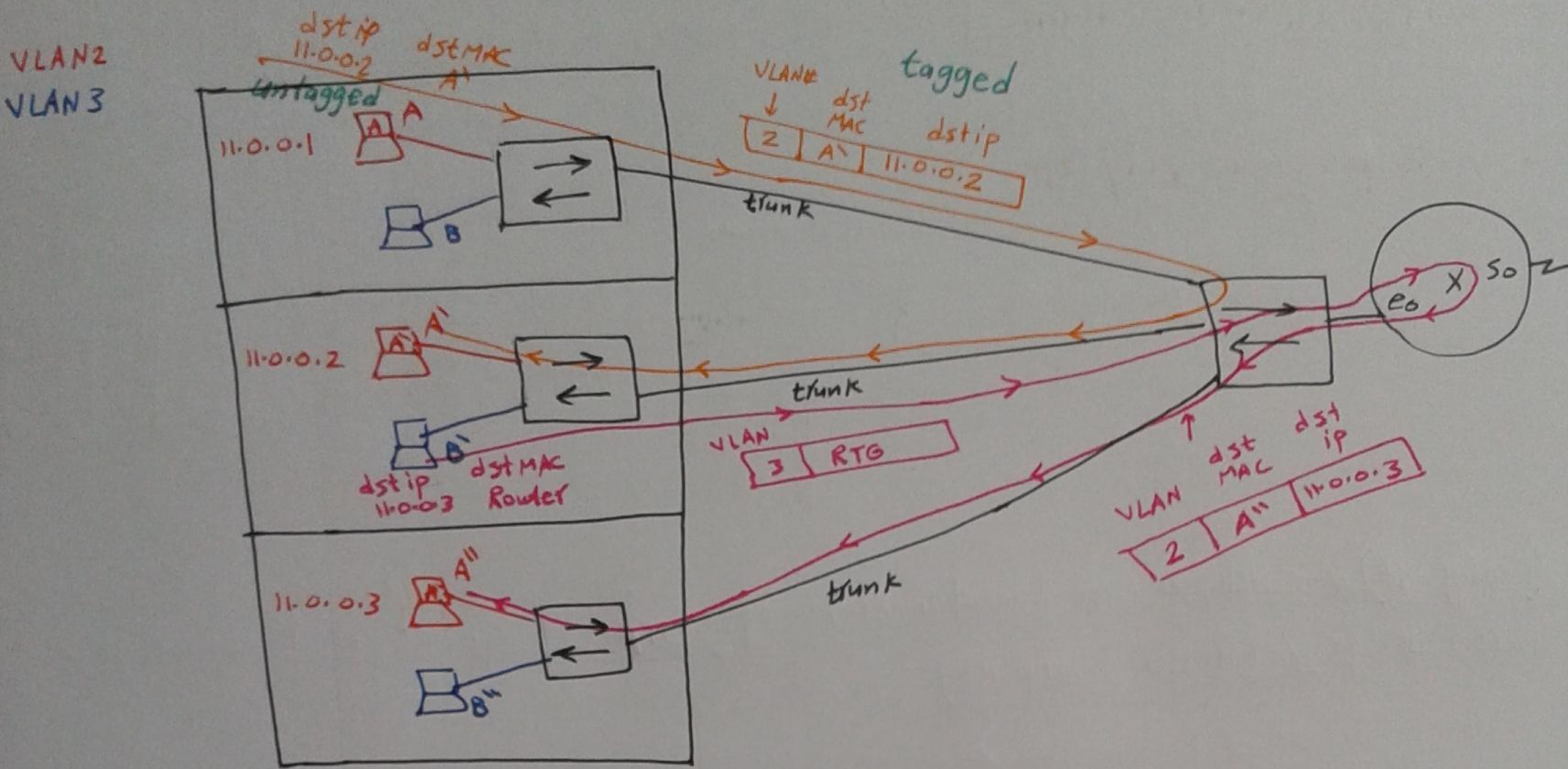
[2] activate VLAN on switch port

(config)# inerface F 0/4
(config-if)# switchport mode access → by defaut port 0/4 will be in VLAN 1 (native VLAN)
→ to change the port 0/4 to a specific VLAN, you can type
(config-if)# switchport mode access VLAN #

[3] configure Trunking & Tagging

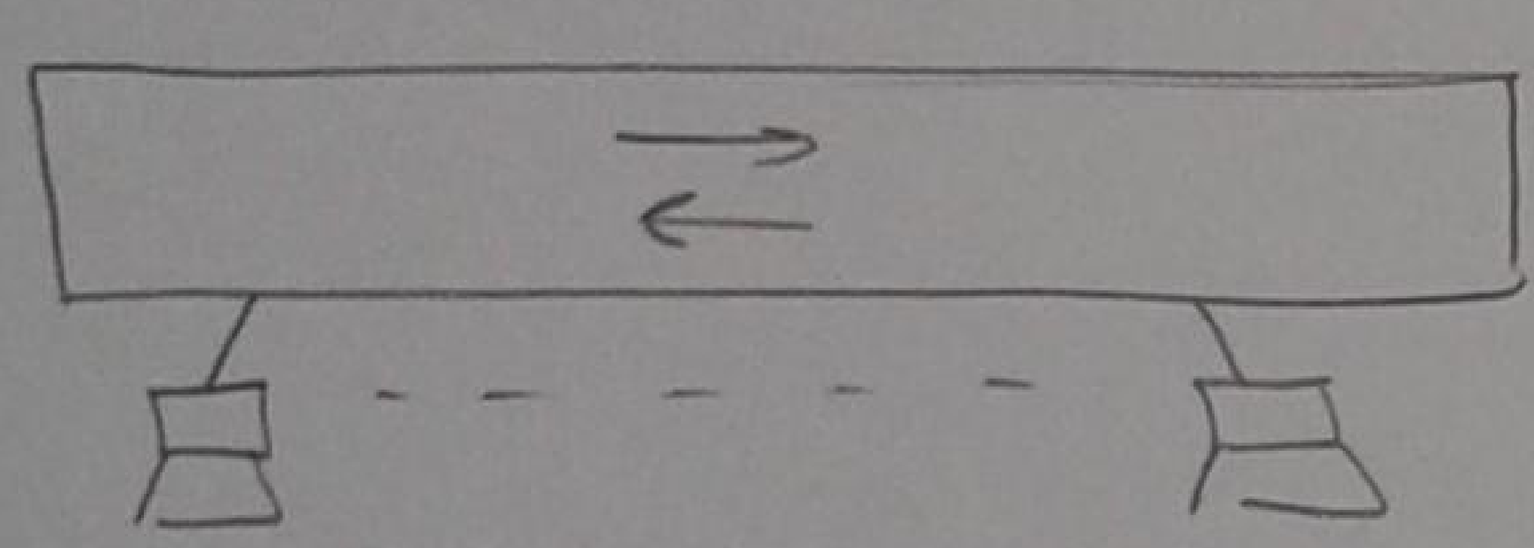
(config)# int f 0/24
(config-if)# switchport mode trunk
→ to choose the tag type [ISL or dot1q], you can type
(config-If) switch port trunk encapsulation { ISL | dot1q } (or)
tag

note/ this order is not written in some switchs like [catlayer3]
because the default tag in it is dot1q



* (Config-If) switch port mode access VLAN ___#___ الامر ده عشان تحدد VLAN معينه لل port

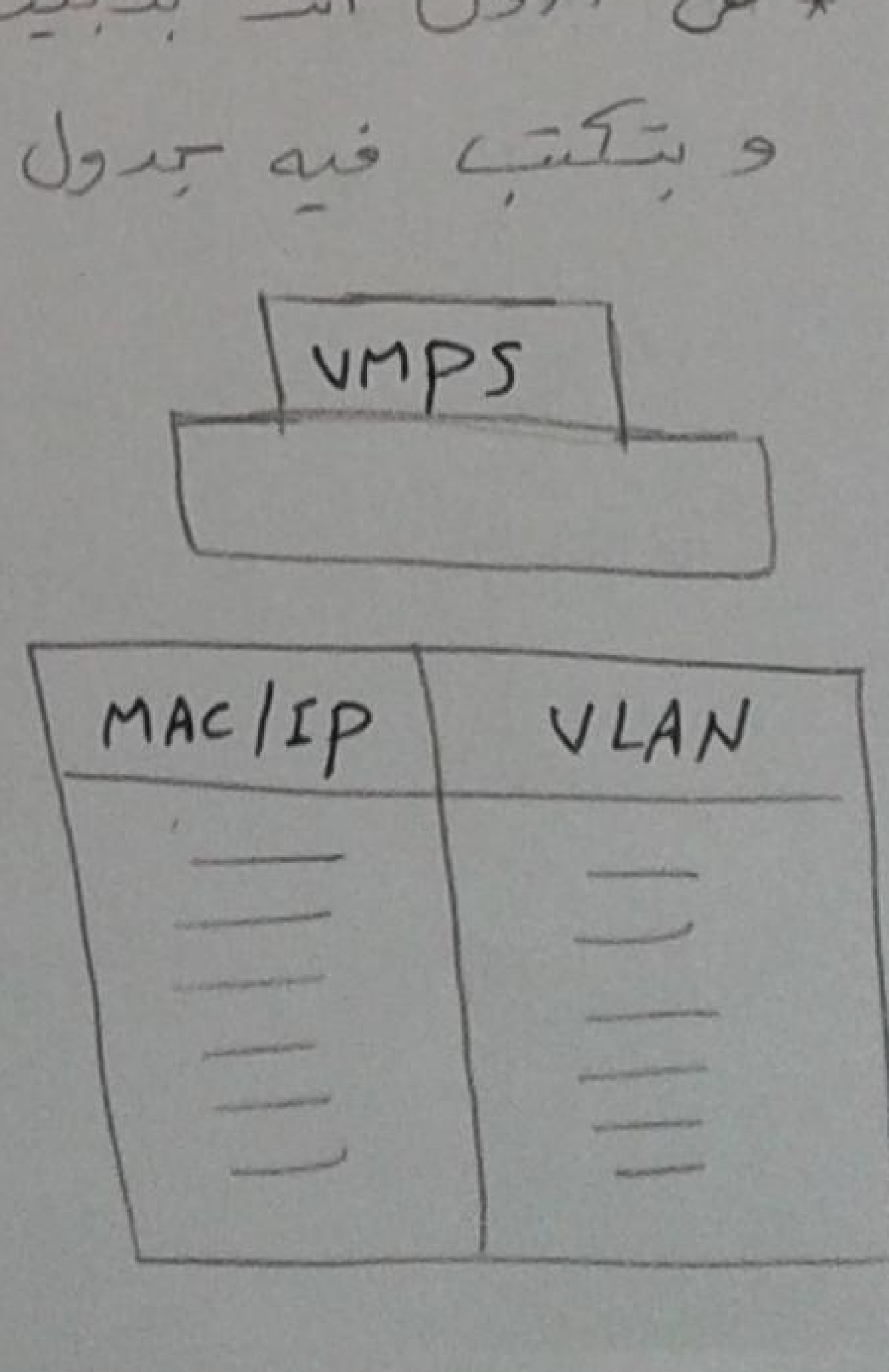
→ Static VLAN membership (98% of usage)
[port Based VLAN]



وهنا انت بتغير ال default VLAN بأيدك من Native VLAN (VLAN1) الى رقم ال VLAN اللى انت عايزها

→ Dynamic VLAN membership (2% of usage)
details in CCIE course
[MAC/IP based VLAN]

* فى الاول انت بتجيب server اسمه VMPS [VLAN Membership policy server] وبتكتب فيه جدول كامل عن كل MAC/IP لكل جهاز وال VLAN اللى بيستخدمه



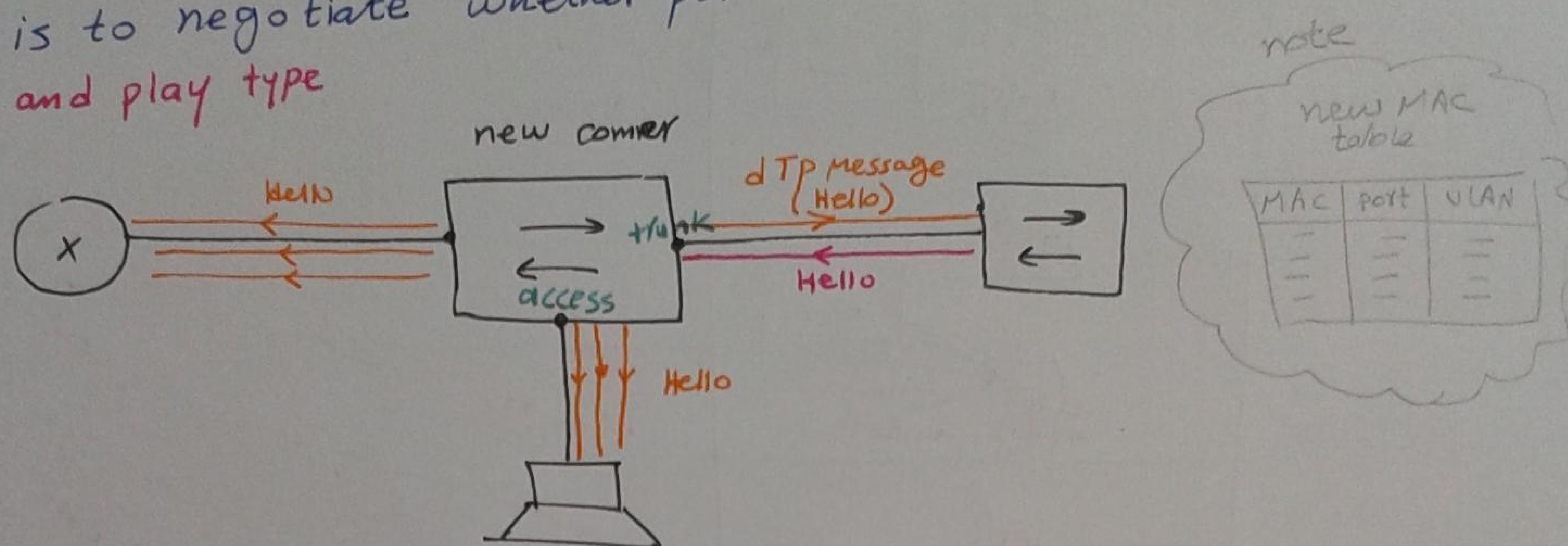
* كل ما DTE يـ connect على ال switch ، ال switch يسأل ال server [ايه هو ال VLAN اللى مشترك فيه جهاز ال MAC او IP بتاعه xxxx]

* وده بيوفر لنا ان ال port مش شرط تكون ثابته فى مكان معين

⟹ this Dynamic membership support security and mobility

DTP : Dynamic Trunk protocol → For cisco switchs only

* it's work is to negotiate whether port should be access or trunk
* it is plug and play type



(Config-If)# switchport Mode {access|Trunk|dynamic} → DTP

* ال Default بتاع اى port بيكون DTP
* اول ما ال switch الجديد بيوصله power هيرسل dtp Msg (Hello) على كل الـ ports بتاعته واللى هيرد فقط بـ Dtp Msg هيعتبره switch ، ويقوم ال switch الجديد بـ configure ال port دى على انه [Trunk port] ⇐ Dinamically

واللى مش هيرد بـ DTP Msg هيعتبرة PC وهيـ Configure ال port دى على انه access port

* المشكلة الوحيدة هنا من ال Router فى انه مش هيفهم DTP Msg وبالتالى مش هيرد وال switch هيعتبر ال port ⇐ access وهى فى الحقيقة trunk

⇐ الحل انى اروح على كل ال ports المتوصله بالـ Routers واعملها config. بأيدى الطاهرة

(config-if) switchport Mode trunk

---

* Managing switch Remotely

(config)# line VTY 0 15 ← يقدر كا واحد يعملوا Telnet للـ switch فى نفس الوقت

(config-line)#password cisco

(config-line)# login

(config)# interface VLAN #

(config-if)# ip address IP Mask ← ال switch هيكون له IP ⇐ وده بنستخدمه عشان ال Telnet بس

(config-If)# no shutdown

(config)# ip default gateway ipof router ← عشان الاخذ والعطا

VTP 33 min lec18

* VTP [VLAN Trunking protocol] for cisco switchs only

- it is responsible for synchorization VLAN Database

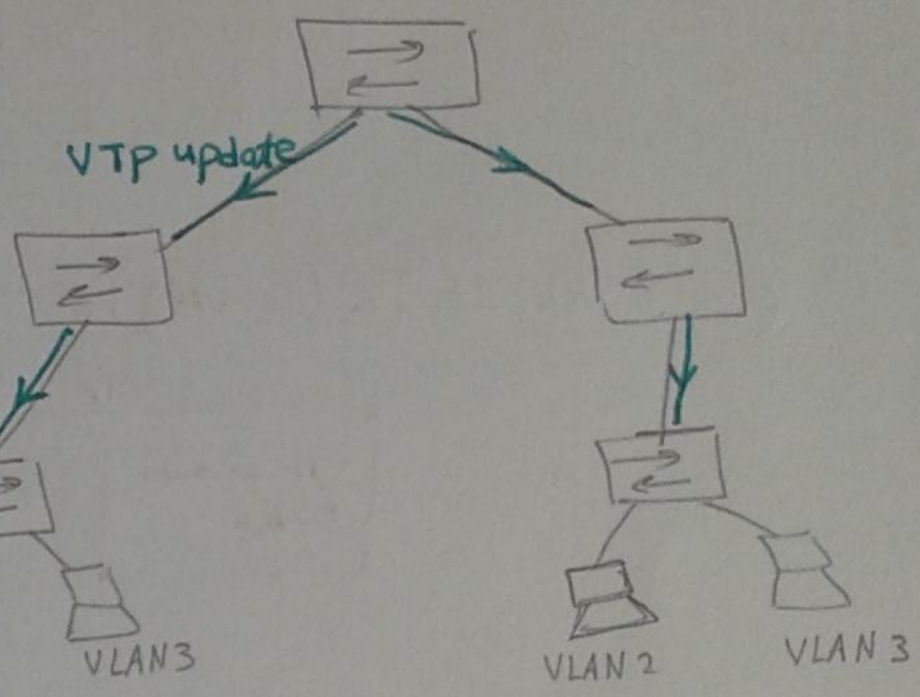
* you can configure any switch [it is not condition the root switch] with VLAN.dat , and this switch will propagate this (VLAN.dat) to all switchs by flooding

note
* If switch doesnot know VLAN , it will drop data
* ~ ~ ~ ~ MAC address , it will Flood data

* VTP conditions for switches that accept the VLAN.dat

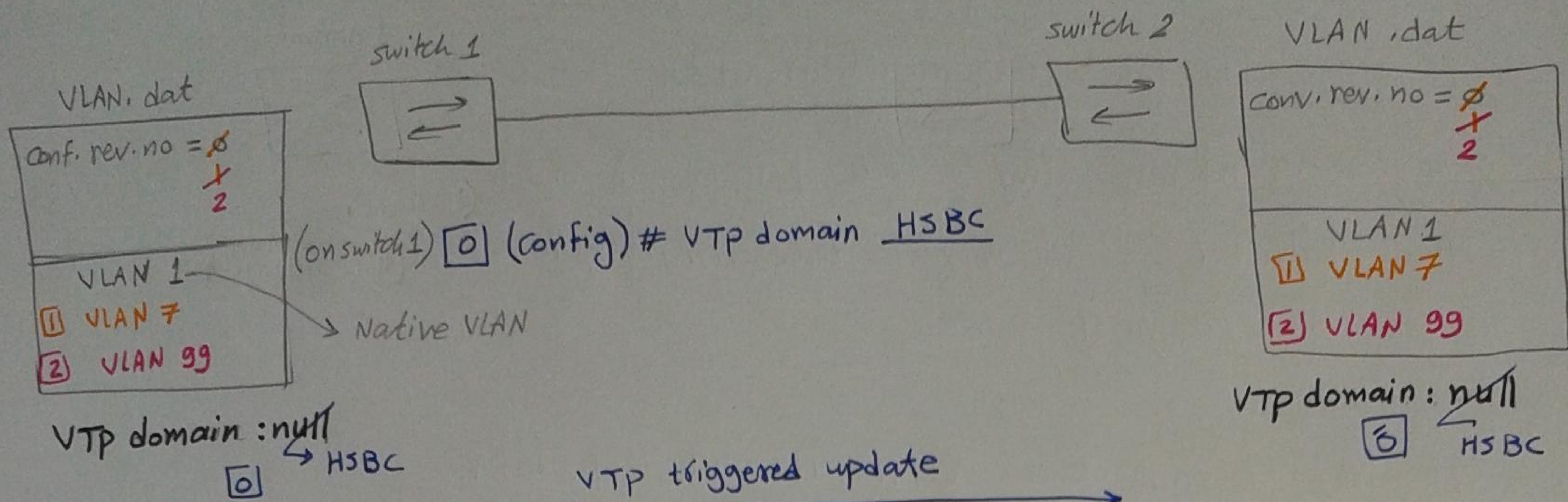
1- Link between switches should be trunk
2- Same VTP domain (AS)

VTp update contains VLAN database



VTP operation :-

* Configuration revision number : is a number that represents the changes [update ما بيحصل لل] that happen in VLAN.dat
* when the switch is new to a network , then the conf. rev. no = 0
* لاحظ انك تقدر configure ي switch وهو بيبعت ال VTp update باقي السويتشات
* the VTP domain name is by default (null) untill you configure it with specific name
* the default of all switchs is server untill you configure it as Transparent or Clinet → it will be explained next
* the Domain Name is case sensitive (ei) HSBC is one domain name & hsbc is another domain name



VTP triggered update →

" VTP domain HSBC "

(on switch 1) [1] (config) # VLAN 7

VTP triggered update →

VLAN.dat	revesion no	VTP domain
1 7	1	HSBC

(on switch 2) [2] (config) # VLAN 99

← VTP triggered update

VTP domain	revision no	VLAN.dat
HSBC	2	1 7 99

* If you want to change the Domain Name to (XYZ), then you have to configure this command [(config) # VTP doman XYZ] in all switches ، every switch at a time (كل switch على حدة)

* step 1 : بعد ما تـ configure VLAN 7 على switch 1 ، switch 1 هيبعت VTP triggered update لكل الـ switches اللى حوليه عن طريق Flooding [فى حالتنا switch 2 بس]

* هنيجى بقى على switch 2 ، switch 2 بيبص على الـ revision number اللى موجودة فى الـ update ويقارنه بالـ revision no اللى عنده ، لو وجد الـ revision no اللى فى الـ update أكبر من (اللى عنده) هيعرف ان الـ VLAN.dat اللى عنده بقت Expired وهيحذفها كامله و يضع مكانها الـ VLAN.dat اللى لسه جايه فى الـ VTP triggered update ، وفى نفس الوقت هيزود الـ revision no بتاعه بقيمة 1

* step 2 زى step 1 بس الفرق الوحيد ان الـ config. كان على switch 2

* فى حاله اختراق ال Network

1) ال pc هيرسل dTp Hello على ال switch

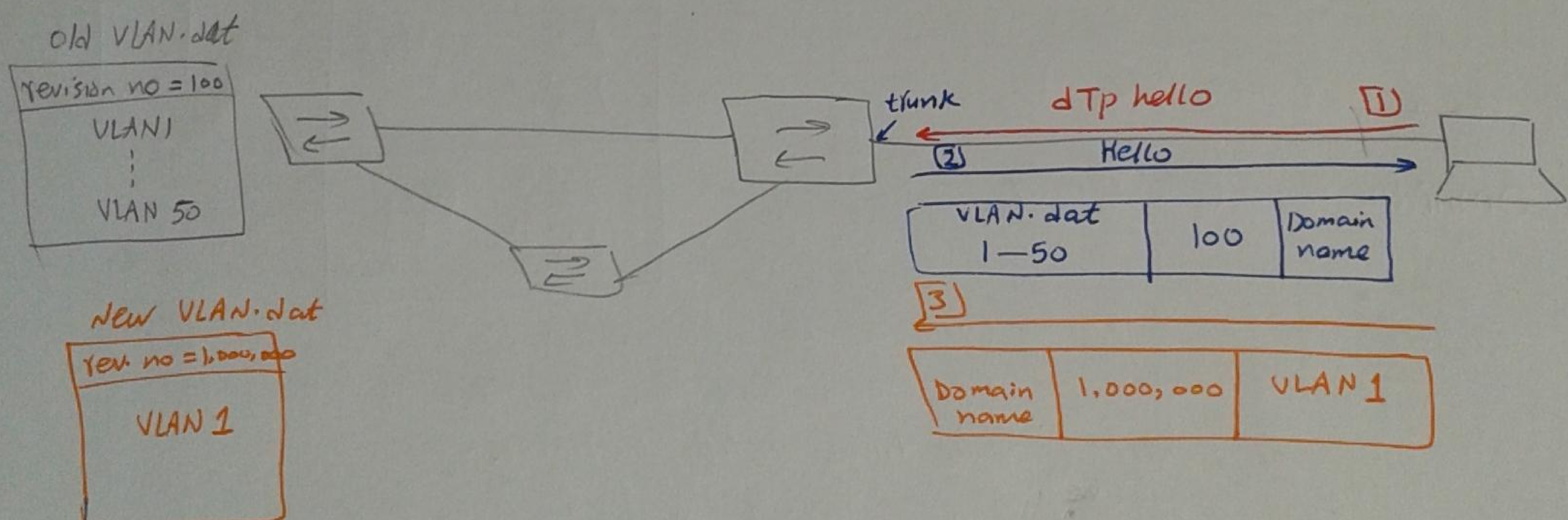
2) ال switch هيعرف ان ال pc ده عبارة عن switch [طالما شاف ال dTp Hello] وهيحول نوع الـ port المتوصله بال pc من ال access الى Trunk وهيبعت VTP update لل pc

3) ال pc هيبعت لل switch ← VTP update بنفس ال Domain name وهيغير ال VLAN.dat وهيكتب فى ال revison no رقم كبير اوى (1,000,1000) مثلا

4) اول ما ال switch هيشوف ال revision no اللى لسه جايه اكبر من اللى عنده ، هيحذف كل ال VLAN.date اللى عنده و هيضع بدلها الجديد [المضروبه] وبكدة اى Data رايحه لـ VLAN معينة ، ال switch مش هيفهمها و هيـ drop ال Data

⟸ كان الحل فى ال command ده عشان يزود ال security ، ولاحظ ان الامر ده لازم تكتبه لكل switch على حده

(config)# VTP password <u>password</u> (option)



---

* (config)# VTP version {1 | 2} ⟹ by default version 1

Note/ Verion 1 & version 2 are incompatible , (ei) all switchs in a single Domain must have the same version

* (config)# VTP mode {server | Client | Transparent}

→ by default server

⟵ ✱ show VTP status

There are three modes that switch can take place

[1] server
* configuration VLAN.dat manually
* propagate VLAN

[2] Transparent
* config. VLAN.dat manually
* by pass VTP updat only

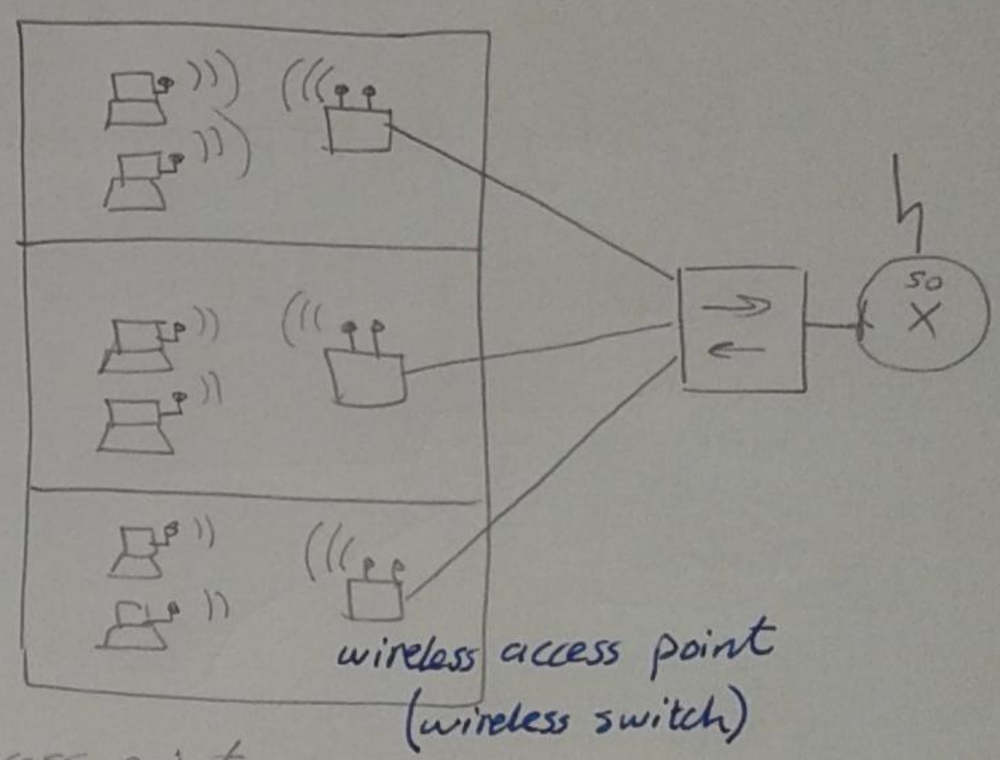
[3] Client
* does not accept any manuall VLAN.dat configuration
* accept VLAN.dat From VTP update only

---

* wifi (wireless lAN)

* the used communication Technology is
CSMA/CA
[Carrier sense multiple Access / Collision Avaidance]

* the used antenna type is
Omnidirectional antenna



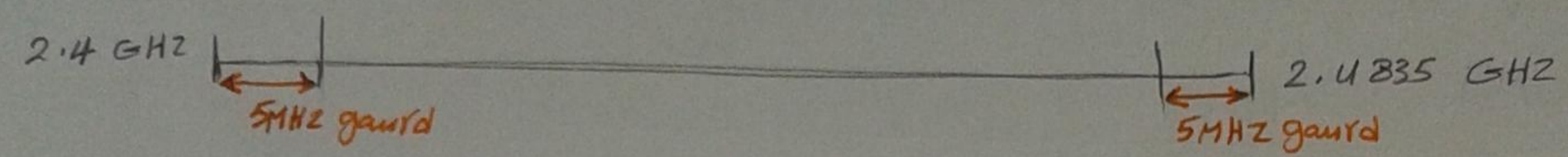
CSMA/CA ⇒ If 3 PCs use the same access point
it makes one PC send and the other PCs are recaiving
or waiting some time untill it finish.

فكره التحفيس في نفس ال Access point مع العلم انهم بتقال السرعه وكمان
بتشتغل Half duplex

Note / لنفترض ان ال Access point بيعطي سرعه 100 Mbps
السرعه اللي ال PC بياخدها بتعتمد على المسافه بينه وبين ال Accesspoint
يعني لو ال PC جنب ال Ap مباشرة هتبقى سرعته 100 Mbps
وكل ما هتبعد ال PC عن ال AP، كل ما السرعه هتقل لحد
ما تقفل لـ No signal

Accesspoint

* there are two bands used for wifi 2.4 GHz & 5 GHz
* 5 GHz is not used in Egypt [in America and canada only]



BW = 83.5 MHz & Chamel width = 5 MHz/ch

∴ no of Channels = $\frac{83.5 \text{ MHz}}{5 \text{ MHz/ch}} \simeq 16$ Ch.

no of ch after Gaurds = 14 ch

---

[2] Wifi standards : IEEE 802.11

(A) IEEE 802.11 B (standard B)

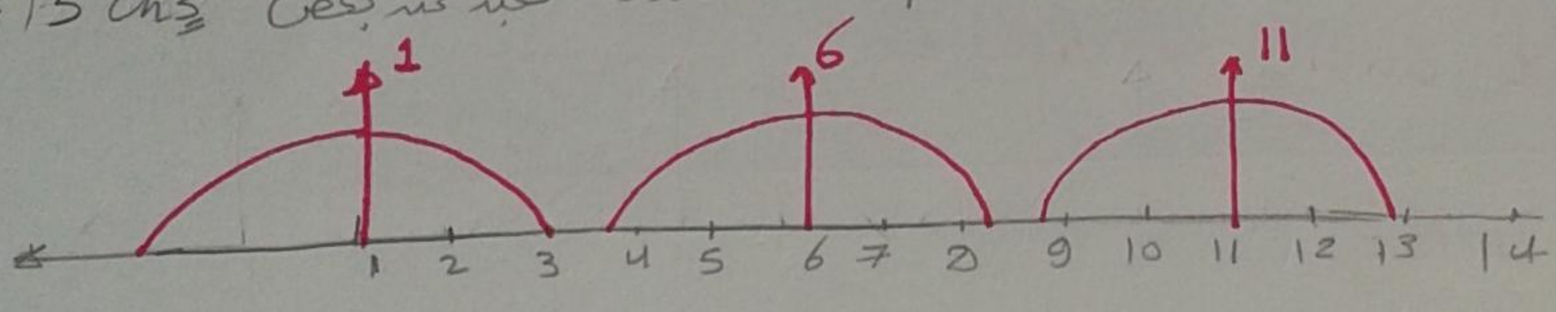
Band : 2.4 GHz

# of Channels : 14 Chs (3 non overlapping area (e.g) 3 only are availabe for usage)

Speed : 11 Mbps

Tx Tequnice : DSSS (Direct sequance spread spectrum)

* لكن لو يكون عندك overlapping ، لازم يكون الـ Frequencies المستخدمه تبعد كم بعض عن الـ 5 Chs



الأول

1 - 6 - 11 ← more usable
2 - 7 - 12
3 - 8 - 13

(B) IEEE 802.11 G (standard G) [used in Homes]

Band : 2.4 GHz

# of chs : 14 chs (3 non overlapping area)

Speed : 54 Mbps

Tx Technice : OFDM (orthogonal Frequency Devision multiplixing)
& DSSS → for standard B

∴ note / standard G is compatible with standard B

ⓒ IEEE 802.11 n (standard N) (الاحدث في السوق)

Band : 2.4 GHZ

# of chs : 14 (3 non overlapping area)

Speed : 108 Mbps ⟶ 384 Mbps

Tx Tequnica : MIMO

ⓓ IEEE 802.11 a (standard A) used in America & Canada only

Band : 5 GHZ

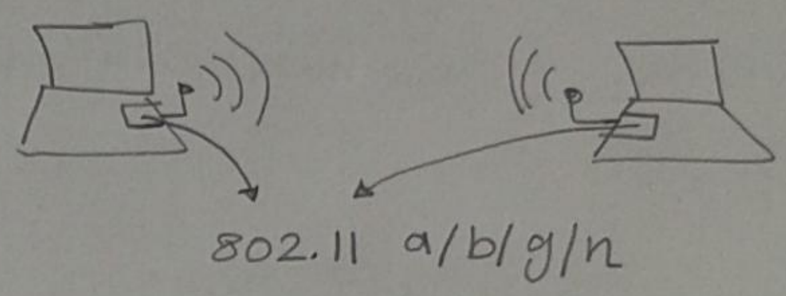
# of chs : 60 (12 non overlapping area)

speed : 54 Mbps

---

* Wifi design

[1] Ad hoc Mode: (point to point) ⇒ اتصال لحظي



non service set

* Access point is called service set also
wireless عدة ال

"IBSS" independent Basic service set

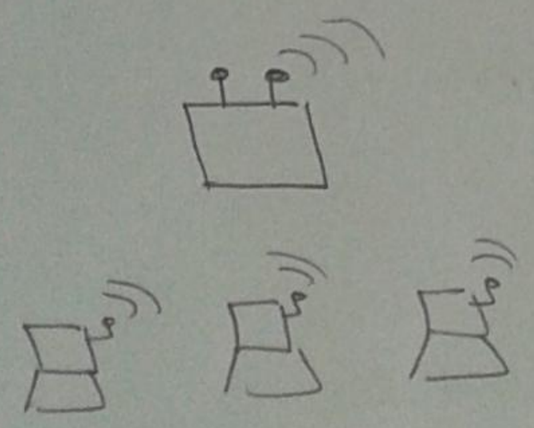
---

[2] Infrastructure Mode: (شبكة ثابتة مثلاً في كافيه او البيت)

Star topology

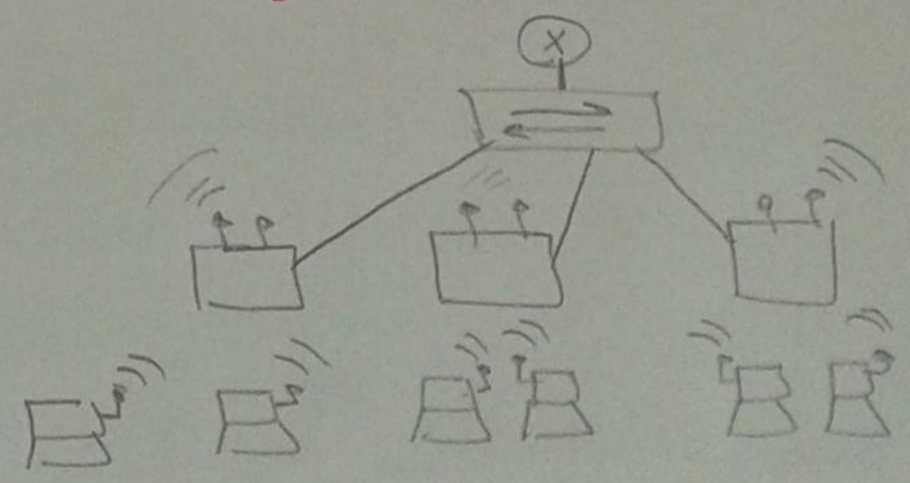
only one access point

"BSS" Basic service set

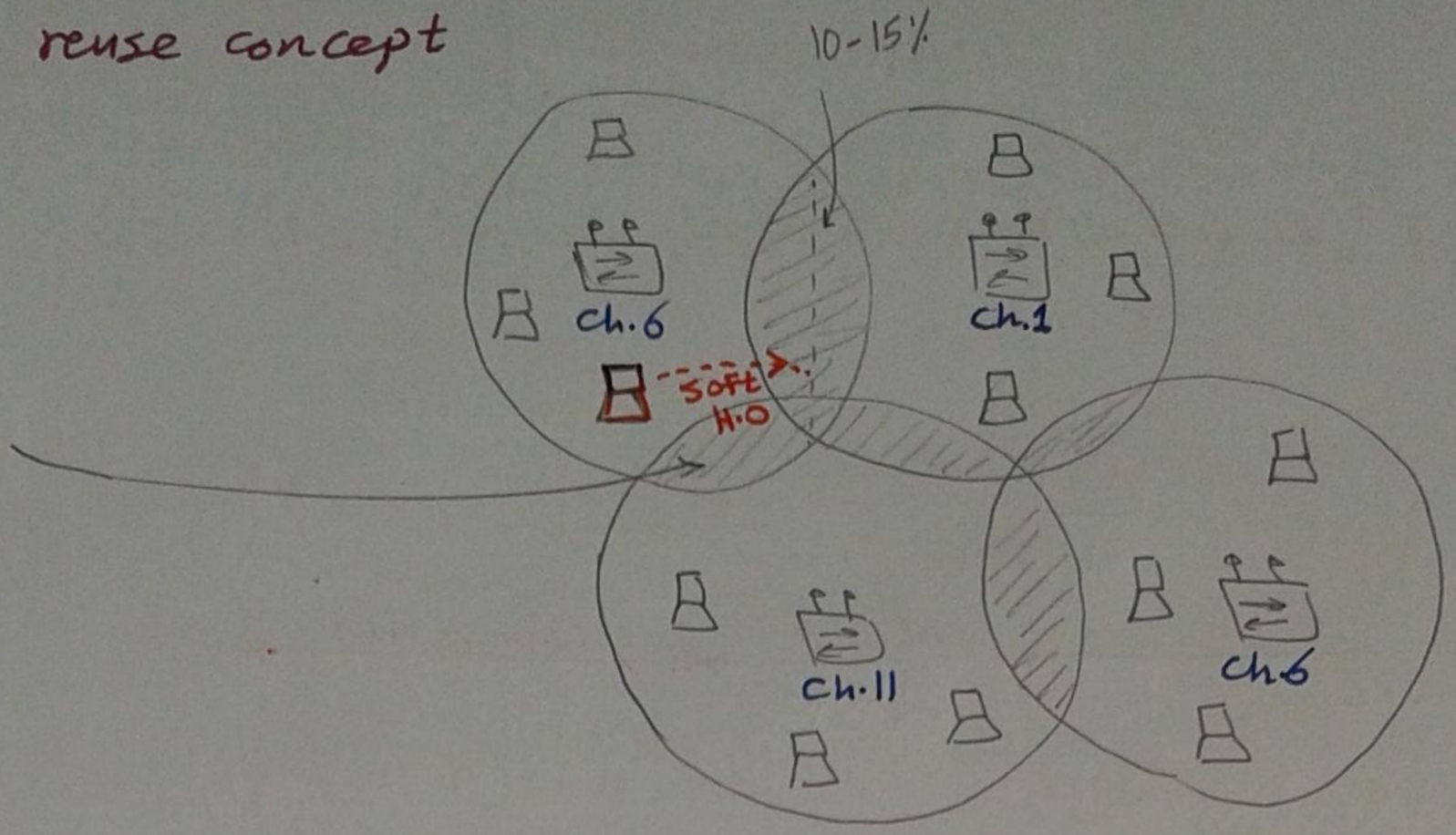


more than one access point

"ESS" Extended service set



Frequency reuse concept

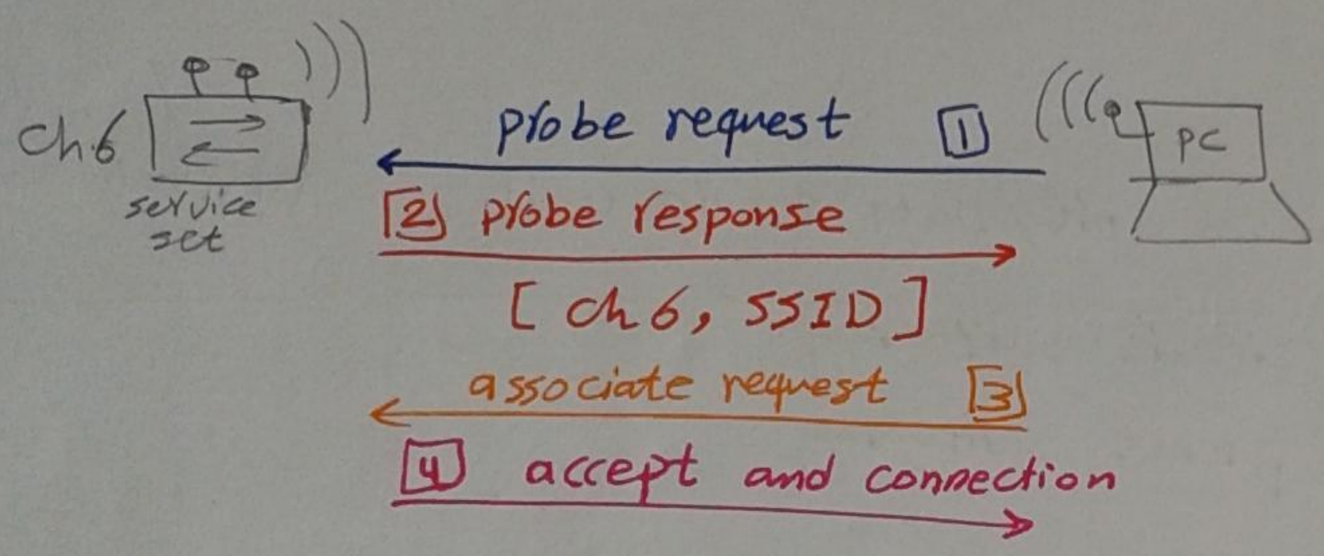


no collition
no interference

---

* The operation of service set while communication with pc

SSID : service set ID (access point بتاع ال (رقم البطاقه) (serviceset)



1 ال pc بيبعت probe request وده عباره عن جس نبض على كل ال available channels
والعمليه دى اسمها (channel scanning)

2 ال service set هيرد بـ probe respone وهيبعت فيها اسم ال channel الخاصه
به وال ID بتاعه

3 ال pc هيبعت associate request وده زى طلب التعاقد بالشبكه (regesteration)

4 Connect & accept

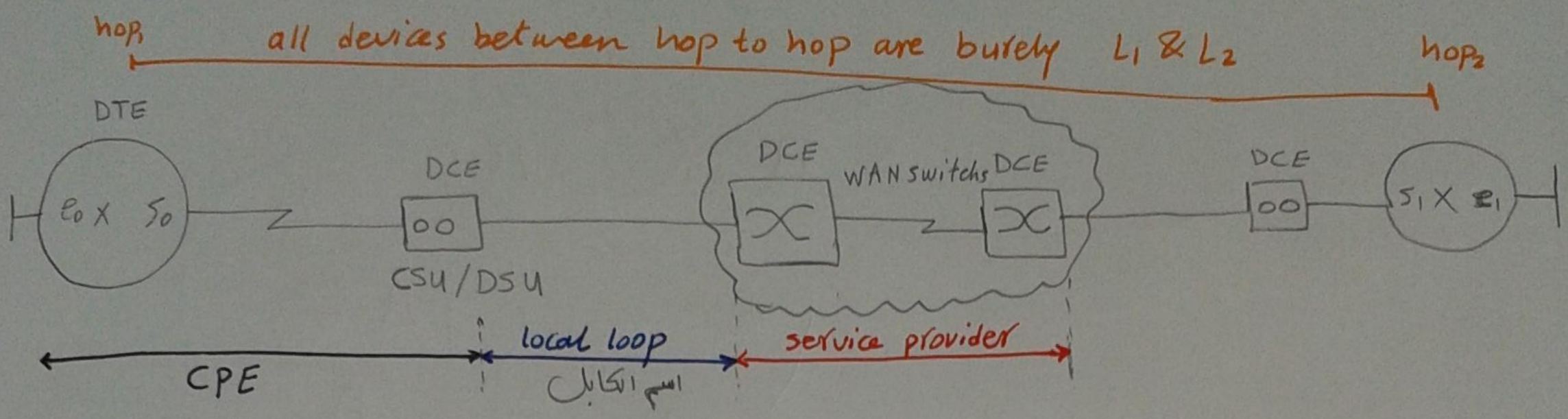
لاحظ / لازم ال pc يكون عارف SSID عشان يقدر ← Network ال, associate
عشان كده ال access point اللى فالبيت بيبعت ال SSID بتاعه فى ال
probe replay و ال access point فى الحاله دى اسمه [public access point]

* ال default على ال access point انها بتعمل Flooding لل SSID بتاعها

* لو ال Ap مش بيذيع ال SSID ← انت لازم تكتب ال SSID بنفسك فى ال PC

الامر على ال pc ← properties ← SSID

WAN switching



* CPE : Costumer premises Equipment [مقر اقامة معدات بتاعة ال Costemer]

* local loop : تبع شركة الاتصالات المحلية زى المصرية للاتصالات وبيكون تحت الارض

CU ↙ ↘ Fiber
<8Mbps >8Mbps

* Csu/DSU : Channalised service unit / Data service unit ⇒ Digital modem

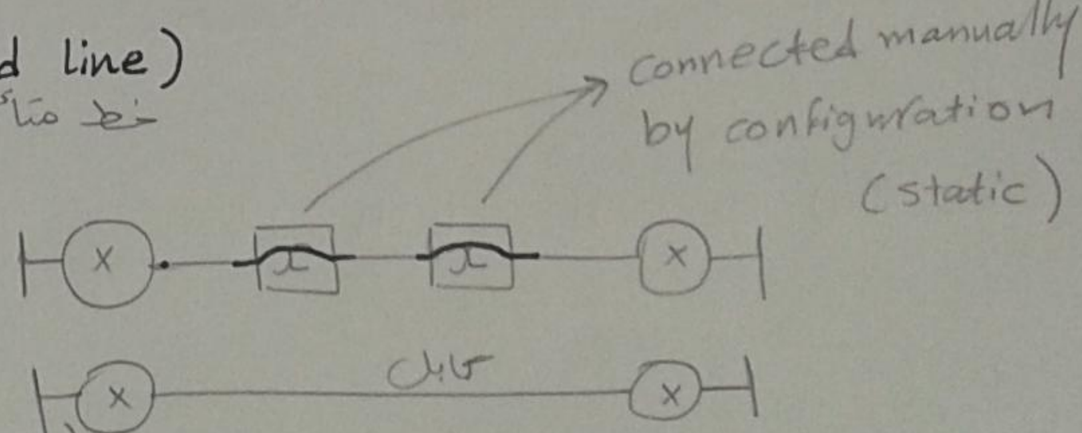
---

* WAN switching → ① circuit switching
→ ② packet switching

① circuit switching (switching before forwarding)

* physical cable from hop to hop where all data moves on the same path point to point

Ⓐ Dedicated circuit switching (leased line) خط متأجر



* it is static line
* 24 hr / 7 day gauranteed link
عيبه انه ايجاره غالى اوى طول الوقت

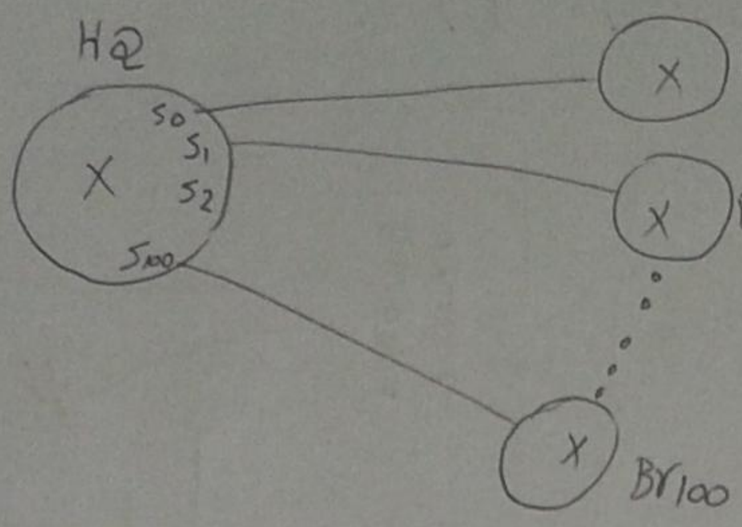
Ⓑ on demand circuit switching (dial up)

* it is dynamic
- analog dial up قديم → 56 kbps
- digital dial up جديد → 128 kbps : 2Mbps ⇒ ISDN [integrated service Digital network]
غالى جدا

anlog or Digital
⇒ Depend on the Modem type

فى الحالة دى انت بتأجر الخط لمدة الاتصال فقط
مش طول الوقت ← اوفر

العيب الخطير لل circuit switching انها بتستخدم point to point only وبالتالى لو انت عندك فروع كتير لشركتك وعايز توصلوا للفرع الرئيسى هتحتاج تأجر خطوط كتير بعدد فروع الشركه ← التكلفة هتكون عاليه جدا



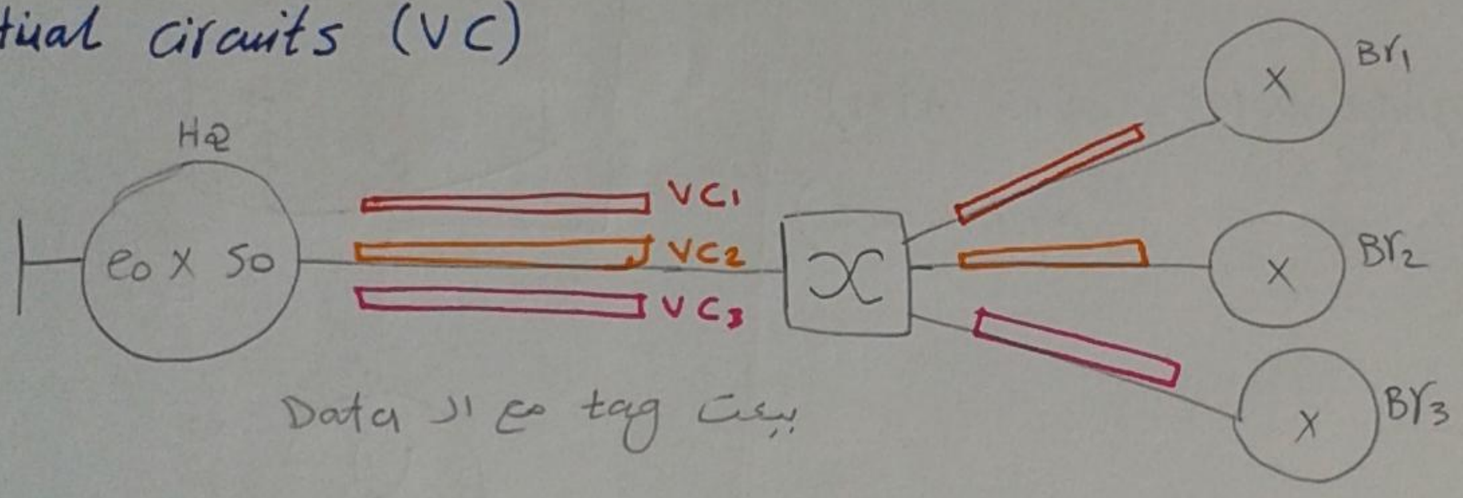
ex. of layer 2 protocols that is used in circuit switching :-

* HDLC
* PPP

---

[2] packet switching (switching while forwarding)

* it is used when point to multipoint switching Topology Based on Vertual circuits (VC)



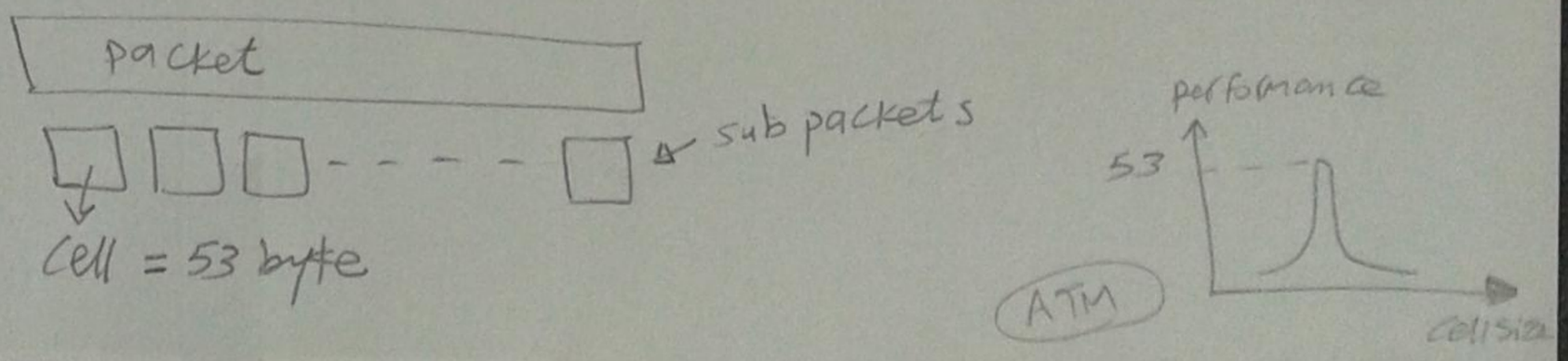
ex: X.25 ⟶ 40 - 45 Kbps → error correction السرعه بطيئة اوى عشانه بيعمل

Frame relay ⟶ 40 - 45 Mbps

ATM ⟶ 40 - 45 G bps → very high cost

(Asyn cronos Transfere Mode)

السرعه الرهيبه فى ATM سببها انه قسم الـ packet الى sub packets اسمها Cell وبالتالى عمل Enhancemat لـ Buffering & processing وحجم الـ cell = 53 byte



Broadband Technology → circuit & packet switching الـ دي غير

it is the use of all Frequencies on the band in order to gain higher speeds

ex: DSL (Digital subscriber line/loop)

* BaseBand Ethernet = 100 m / 1 Gbps
* BroadBand ~ = Modulated Ethernet
= 10 km / 8 Mbps

* DSL is L_1 not L_3

Because it is Modulator demodulator only Between BaseBand Ethernet and BroadBand Ethernet

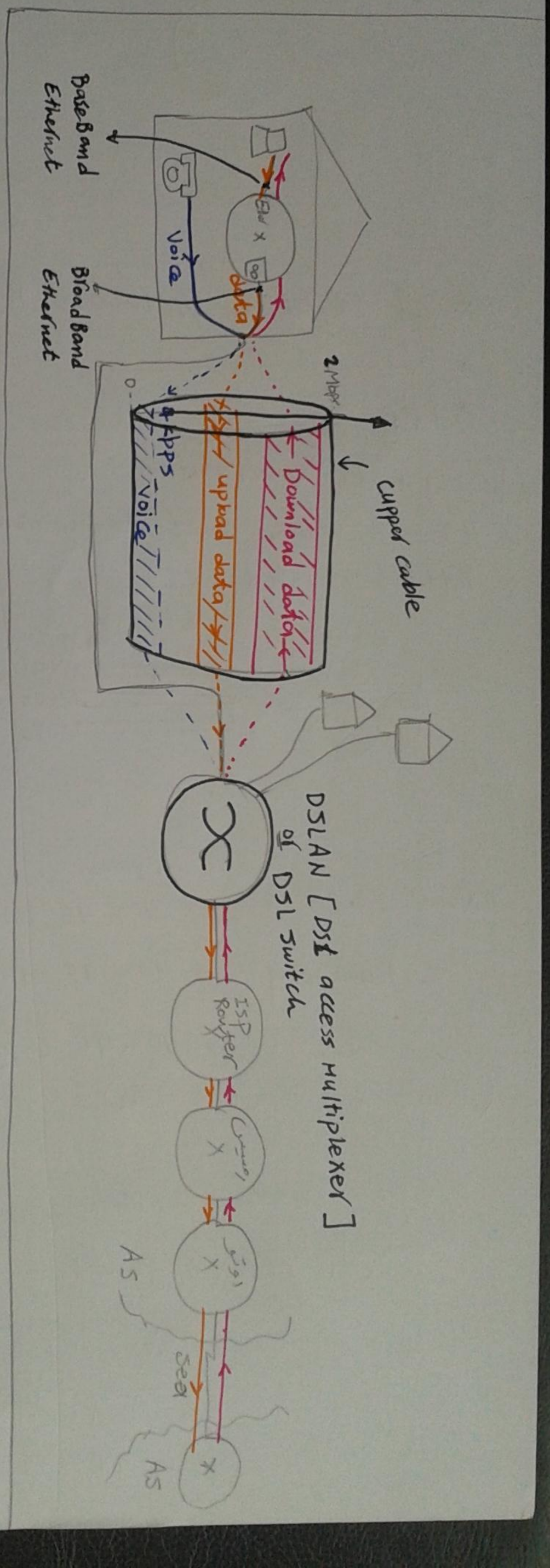
* DSL has the advantage of CS & PC

مميزات الـ دي

L_2 protocols

* L_2 : PPPoA (point to point protocol over ATM)
: PPPoE (~ ~ ~ ~ ~ Ethernet)

* L_3 : IP/static

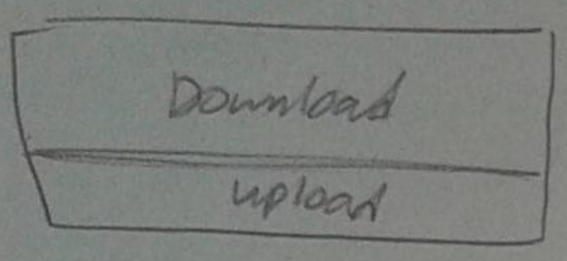


اسم العائلة DSL

ADSL
(Asymetric DSL)

Download > upload

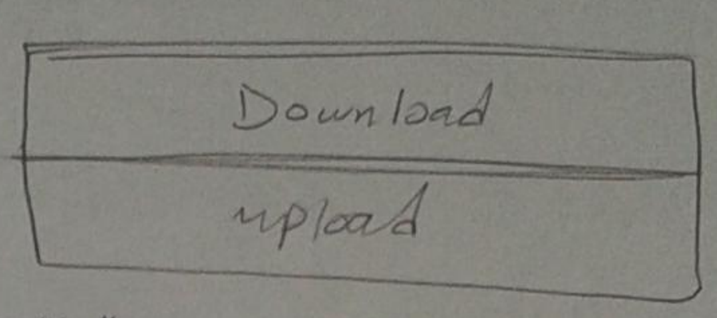
* used for Home users



SDSL
(symetric DSL)

upload = download

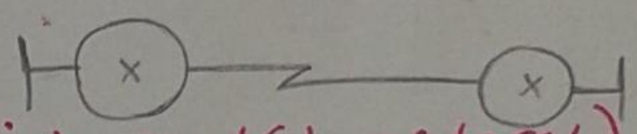
* used for Enterprises



بيل ما الشركه تأجر (leased line) اللي هو
نالي دي ← بتشتري SDSL

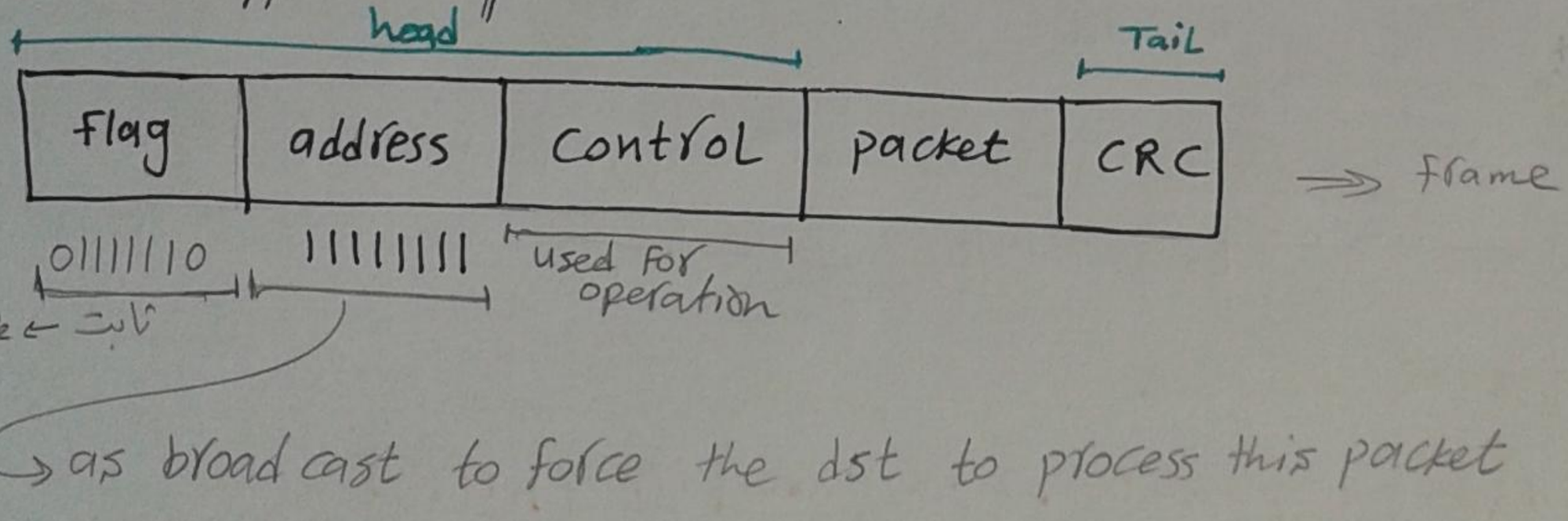
Circuit switching protocols

ⓐ encapsulation

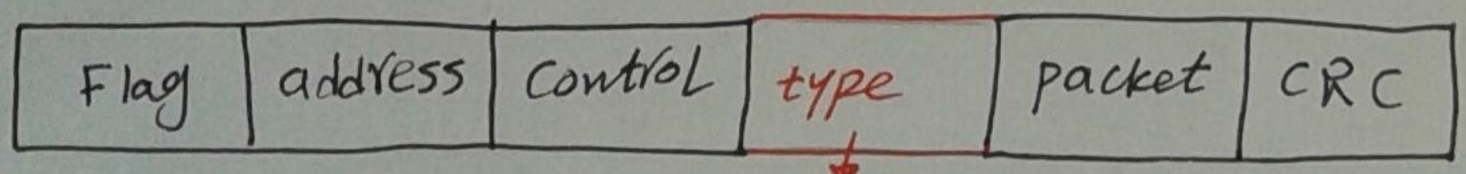


ISO HDLC (High level Data link control protocol)

it is not supported by cisco



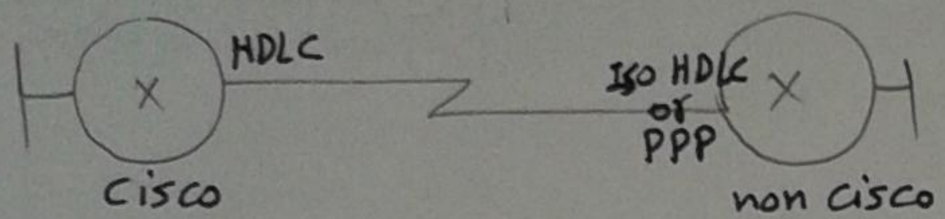
CISCO HDLC (٪1 of usage)



type : it contain upper layer protocol

Note / HDLC is L2 protocol

* the Default of cisco routers in L2 is HDLC protocol and you can change it by configuration

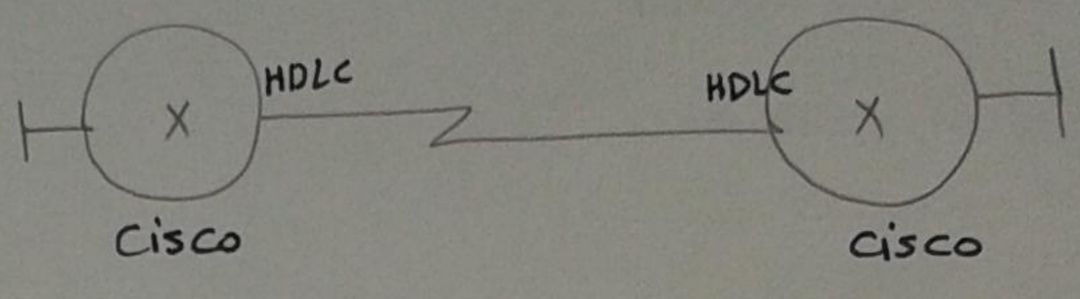


show ip interface breif

status	protocol
L1	L2
up	down

الروترين مش قادرين يعملوا L2 protocol

الحل في PPP

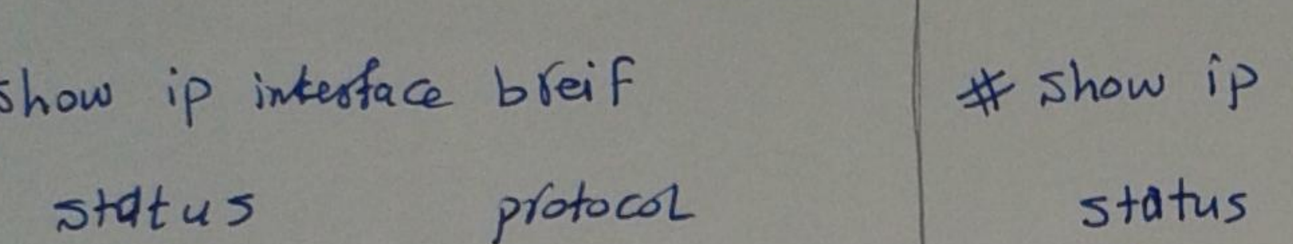


show ip interface breif

status	protocol
L1	L2
up	up

* PPP (point to point protocol) ⇒ Standard ⇒ اللي اخترعه الـ IETF وده صيغة تاني الـ IEEE

(99% of usage)

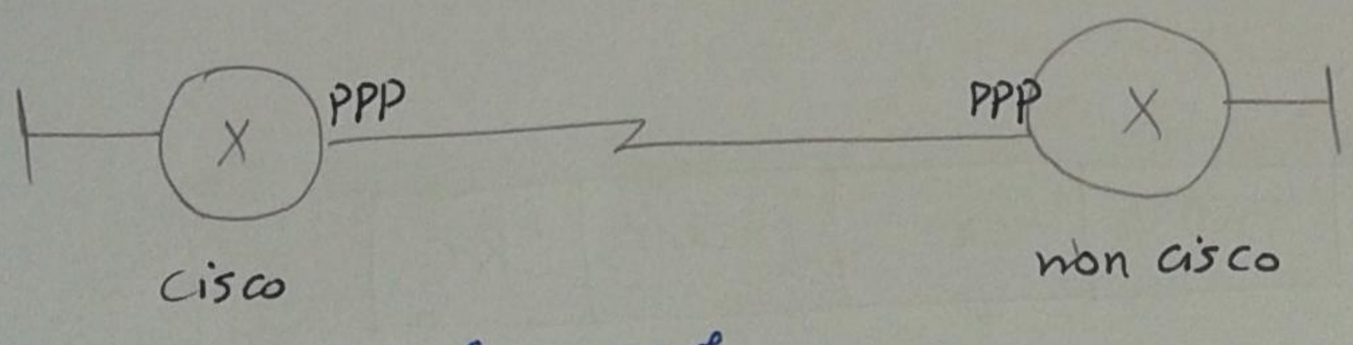


نفس شكل الـ HDLC Frame بتاع cisco بس بأكواد مختلفة

* دلوقتي عشان طريقة الـ configuration تفكر تغير الـ cisco HDLC اللي هو الـ Default بقى وبالتالي PPP L2 protocol بقى روا يفهموا non cisco & cisco routers

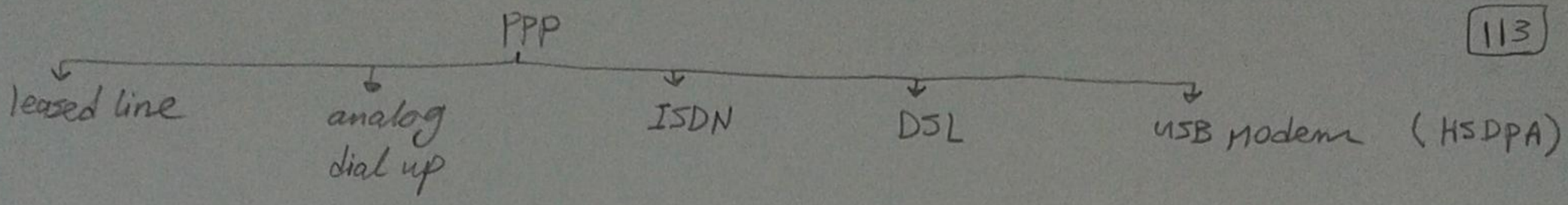
(config)#int s ____

(config-if)# encapsulation { FR | X.25 | PPPOE | PPP } (or, or, or)



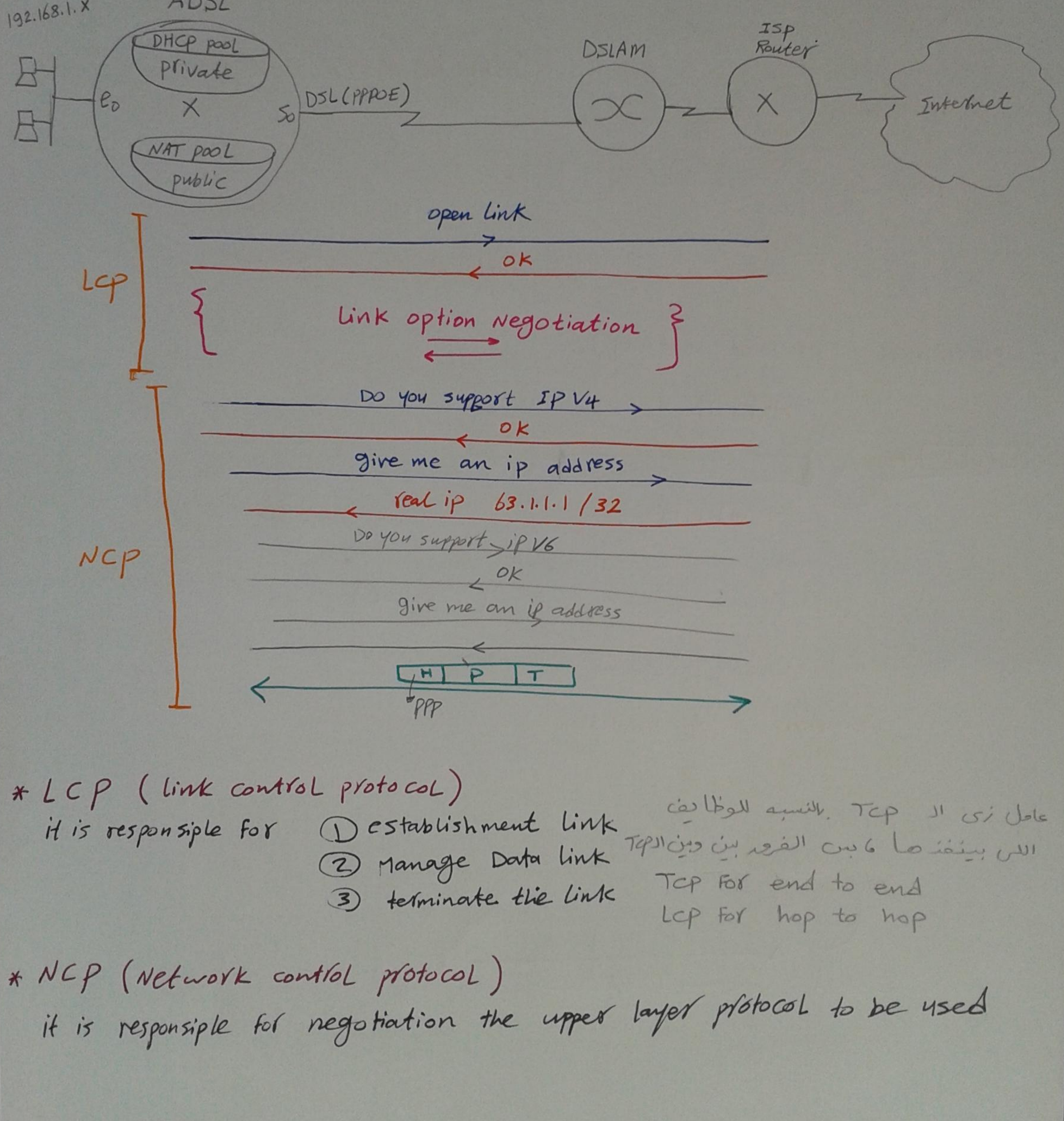
show ip interface breif

status	protocol
L1	L2
up	up



* PPP operation

to see the operation live press [# debug ppp negotiation]



* LCP (link control protocol)

it is responsiple for
1. establishment link
2. Manage Data link
3. terminate the link

عامل زى الـ TCP بالنسبه للوظايف اللى بينفذها بس الفرق بين وبين الـ TCP

TCP for end to end
LCP for hop to hop

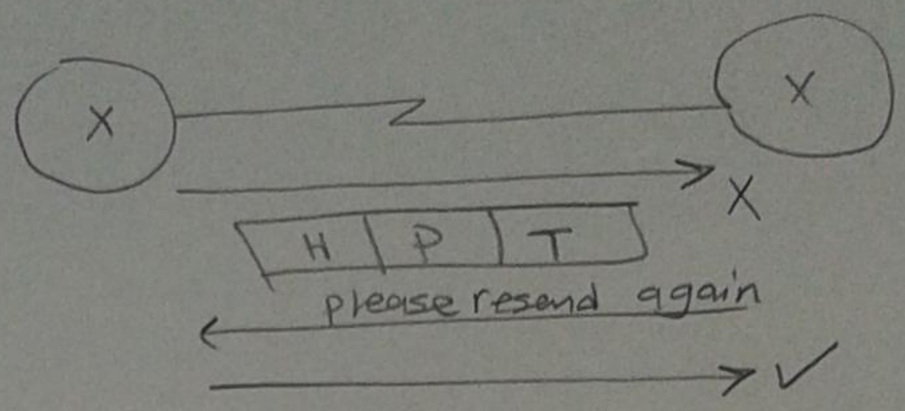
* NCP (Network control protocol)

it is responsiple for negotiation the upper layer protocol to be used

* PPP option negotiation

[1] error correction

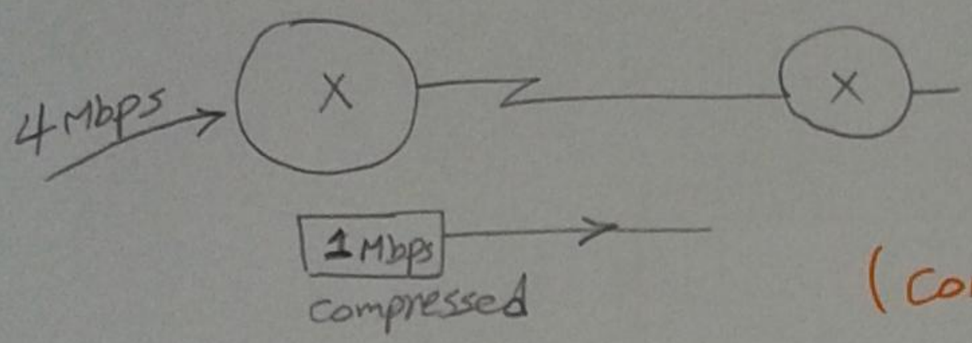
هنا الـ Router يوقع الـ Data هو اللى بيطلبها قبل ما توصل لـ PC



لاحظ / الروترين لازم يـ support نفس الـ option عشان يشتغلوا

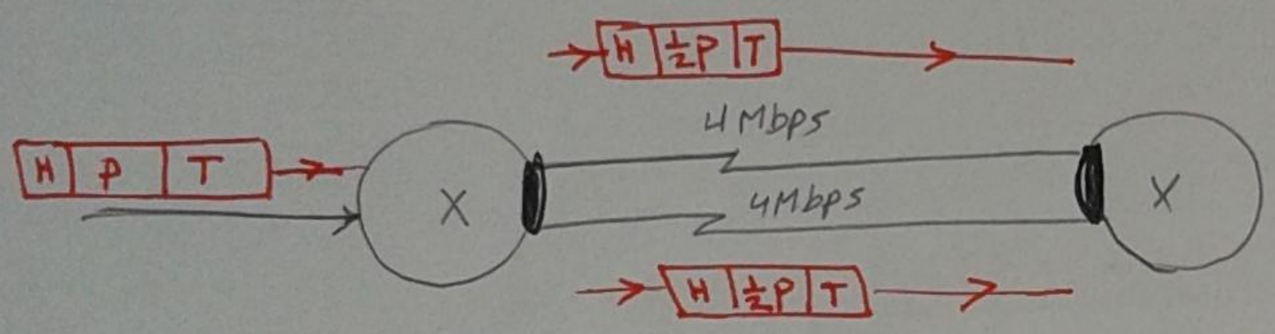
(Config-if) # PPP collection

[2] compression



(config-if) # PPP compression

[3] Multilink (as load sharing)



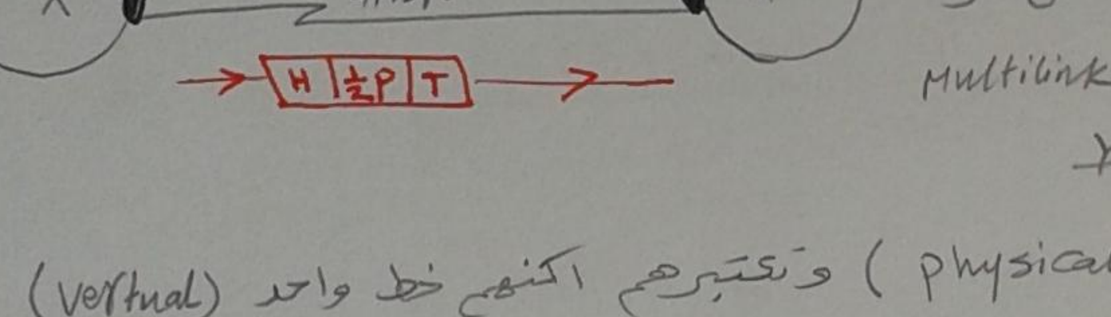
لو انت عايز سرعه 8 Mbps والنحاس اقصى سرعه 4 Mbps ← الشركه بتعملك الـ Multilink وهو زى الـ load sharing بالضبط

⇐ الشركه بتعجزلك خطين (physical) وتعتبرهم اكنهم خط واحد (Vertual)

الـ packet بتيجى عند الروتر الاول هيقطعها نصين ويعطى لكل نص (Head + Tail) ويبعتهم

(config-if) # PPP Multilink

[4] Call Back



5 cent / min

10 L.E / min

عشان يتحاسب بالتعريفة الاقل

(Config-If) # PPP call Back

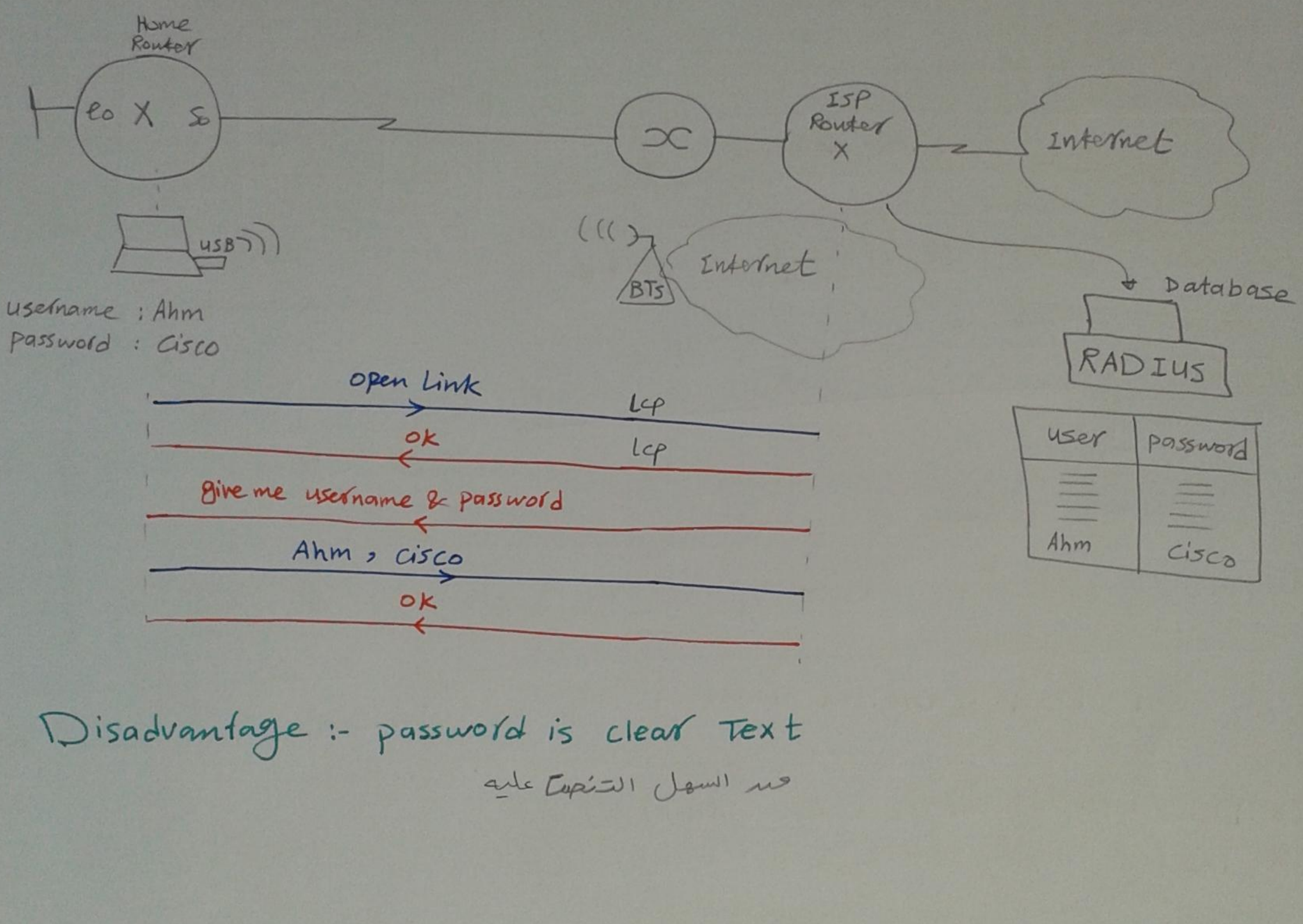
5 Authentication (username & password)

(config) # int S0

(config-If) # encapsulation PPP

(config-If) # PPP authentication { pap | chap }

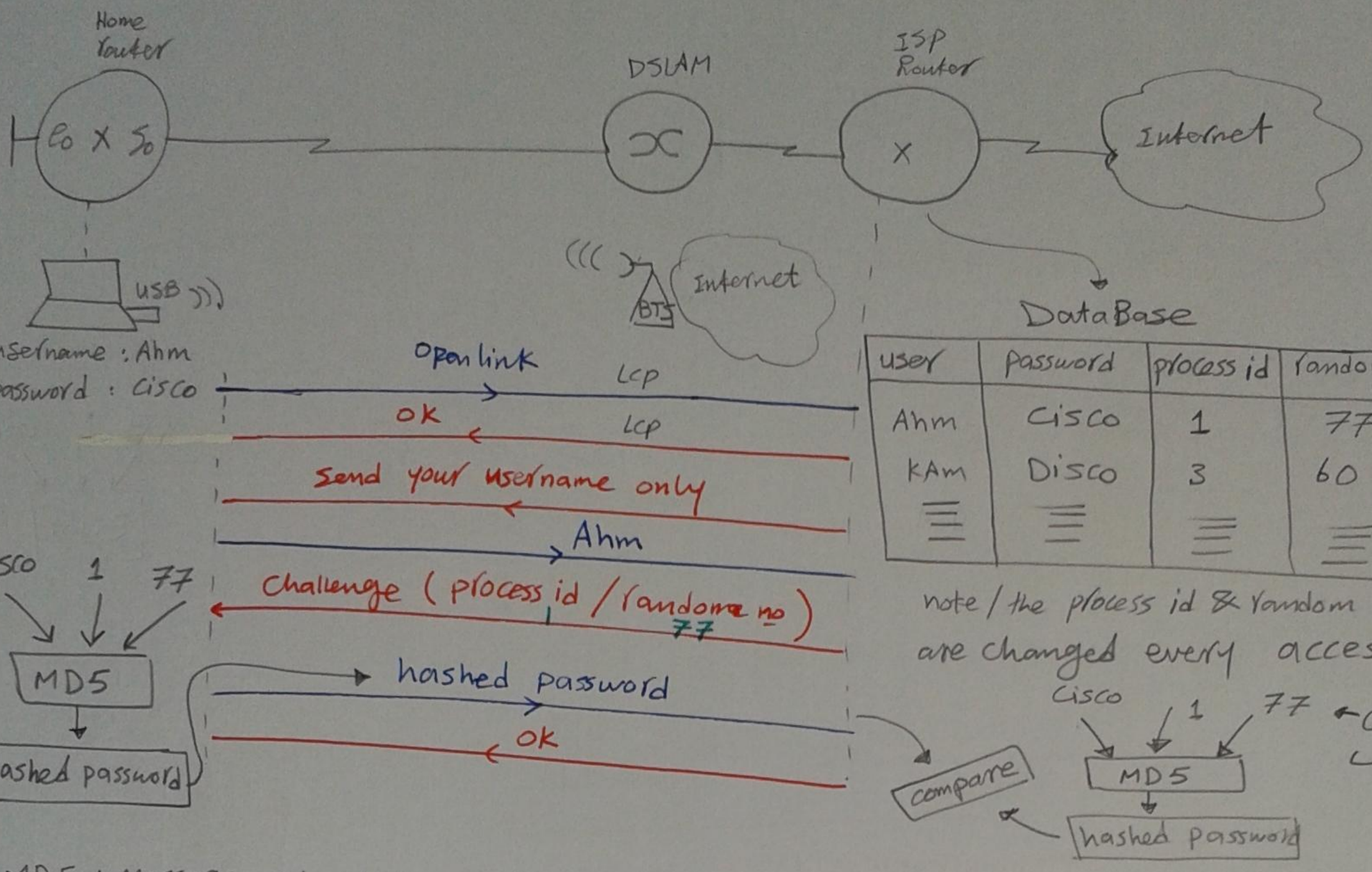
A PAP (PPP Authentication protocol)



Disadvantage :- password is clear Text

عيب السهل التنصت عليه

[B] CHAP (Challenge Hand shake Authentication protocol)

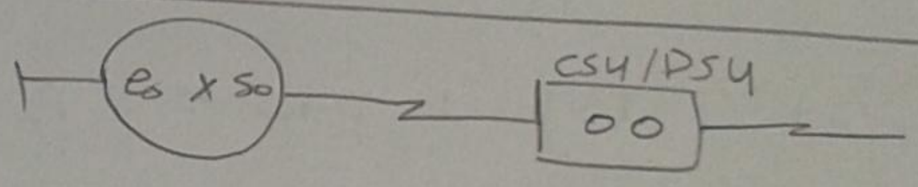


MD5 : Message Digester 5 (it is one way function)

pass. تعرف الـ ← منقدرش hashed pass & MD5 يعني لو انت عارف الـ

---

* CSU / DSU [Digital Modem]



* DS0 : Digital service zero (64 Kbps)
* DS1 : Digital service 1

T1 (أمريكا وكندا) — E1 (أوروبا)

24 DS0 = 1.54 Mbps

32 DS0 = 2 Mbps

* DS3

T3 — E3

45 Mbps — 34 Mbps

* STM 1 ← بتستخدمه مد سنترال اوتو الى اوروبا

155 Mbps

STM2 = 3, 4, ...

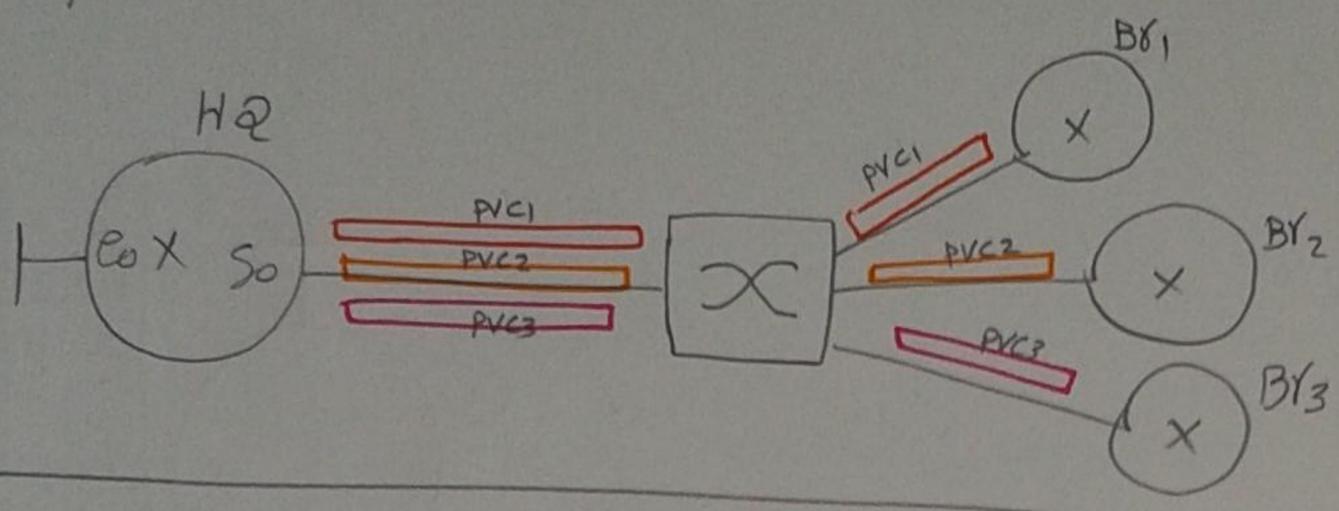
10 Gbps

packet switching

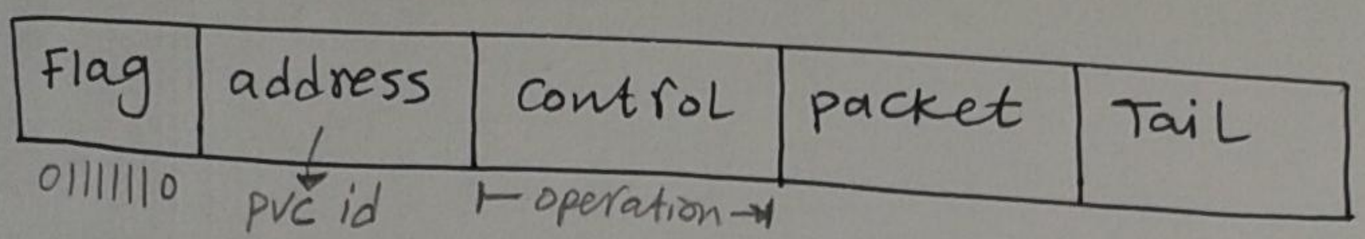
EX: FRAME RELAY → X.25 سرعاته بطيئة جداً والـ ATM الاكثر استخداماً لأنه الـ غالي اوي

it is point to multipoint packet switching based on PVCs

PVC : permenant vertual circuit

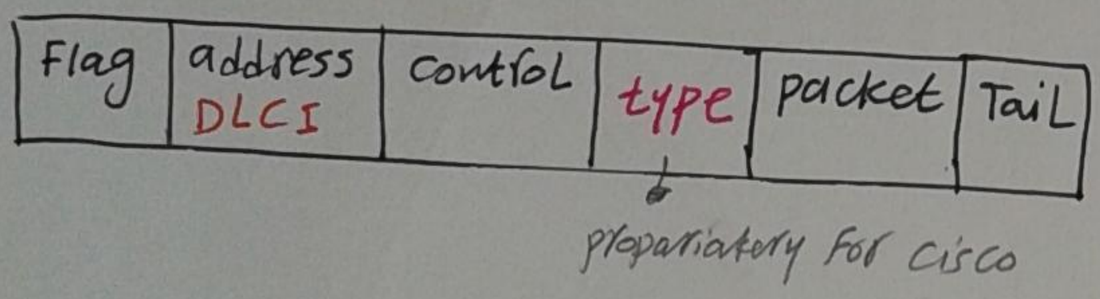


FR encapsulation *is called LAPF (link access procedure for fR)
protocol

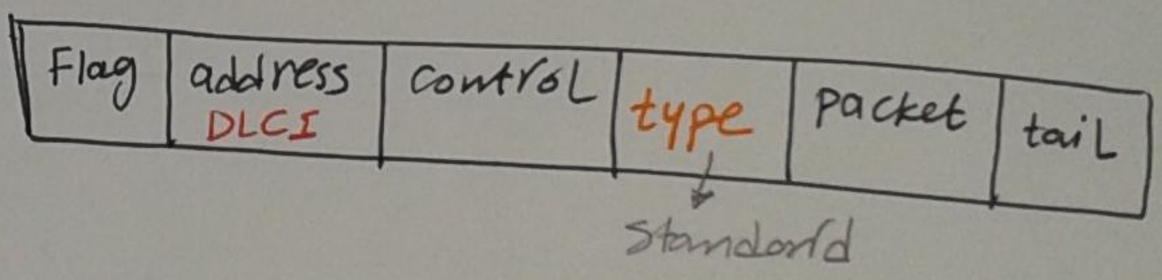


زي الـ ISO HDLC بالضبط

Cisco LAPf



IETf LAPf



*address

X.25 → X.25 no → PVC id (8 bit) ↔ 0 … 255

يعني انك ممكن تعرّف 256 PVC على نفس الـ physical cable

FR → DLCI (Data link circuit identifier) → PVC id (10 bit) ↔ 0 … 1023

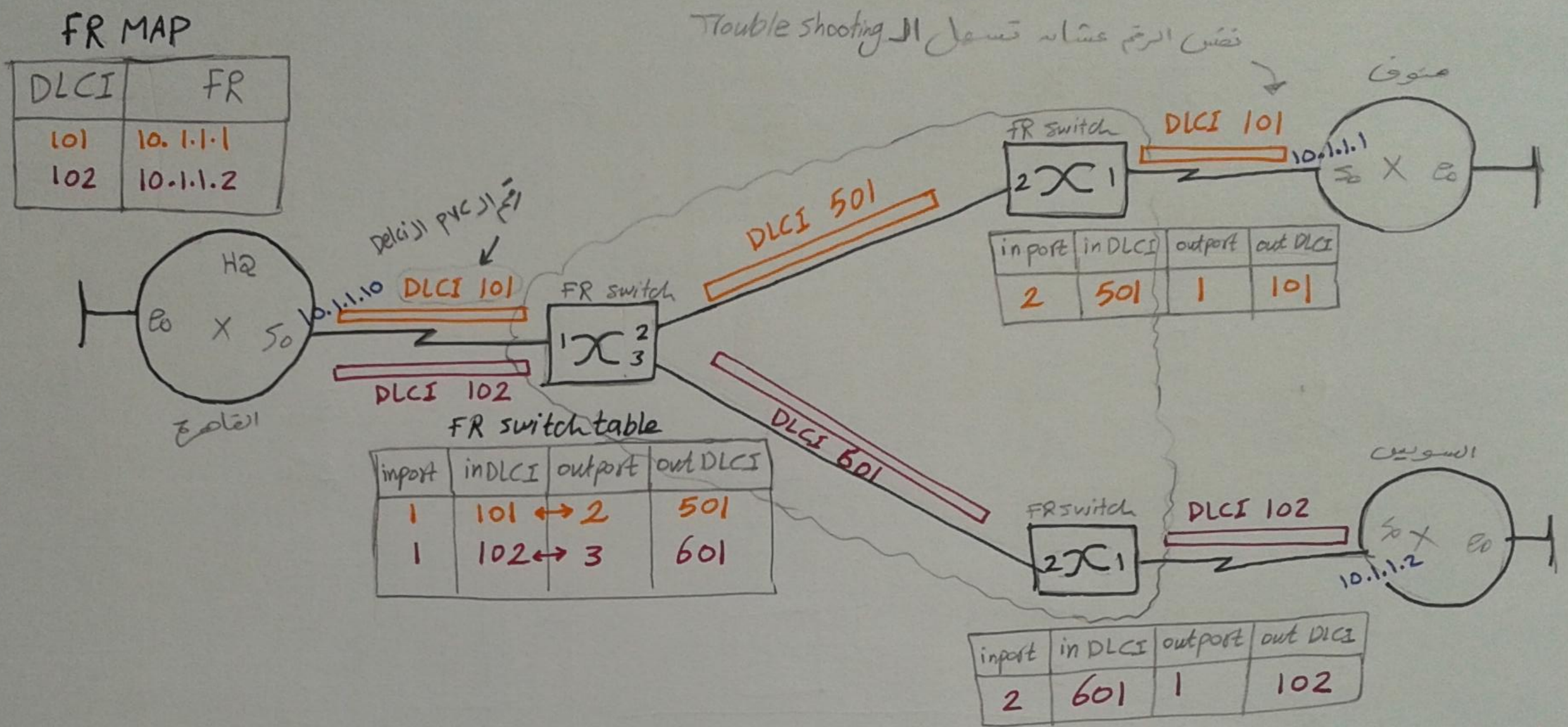
ATM → VPI/VCI (vertual path id / vertual circuit id) → PVC id (16 bit) ↔ 0 … 65535

FR operation steps:-

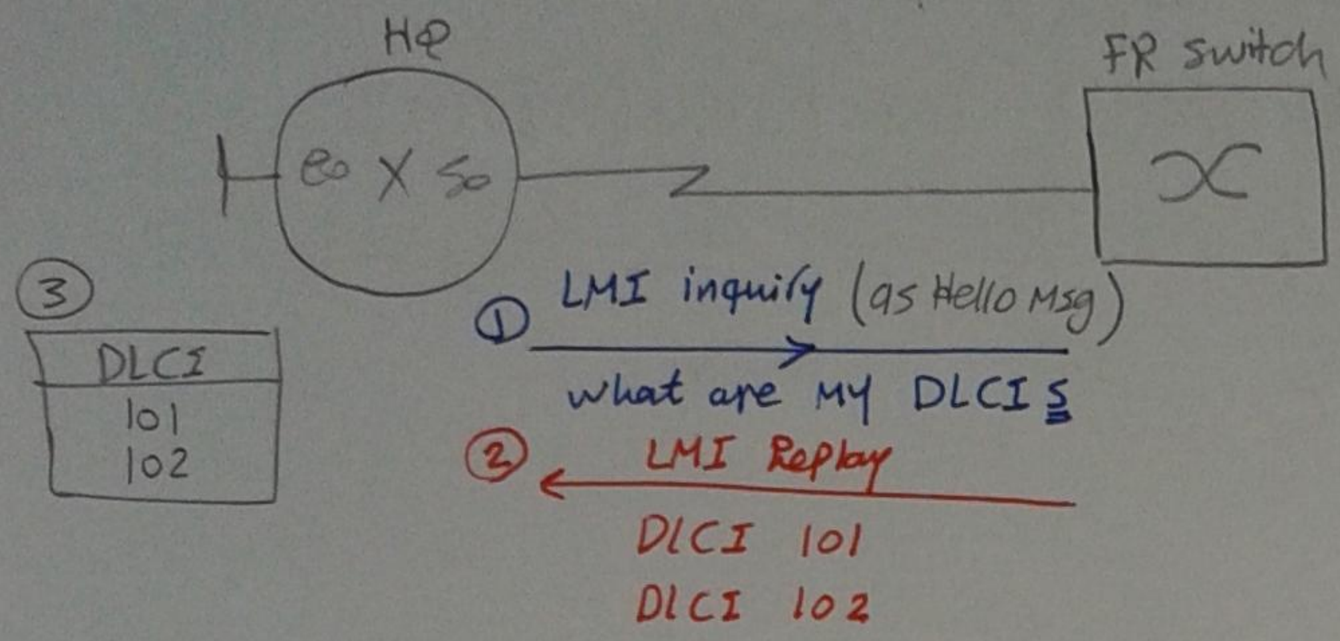
1- FR switch statically configures its PVCs using LMI

2- FR router dynamically discovers its PVCs using IARP

3- FR router dynamically map DLCI to next hop router using IARP



* The second step is LMI operation
  * LMI (local Management interface)
  * it is as hello msg to be sure that the PVCs are keepalives



[active يعني ال PVC شغاله من الطرفين والسكه كلها سليمة]

[inactive يعني ال PVC سليمة جنبي لكنه من فصل او قطع بعيد عني] ← يكتب جنب DLCI

[Deleted يعني ال PVC اللي جنبي مباشرة failed او ال connection فاصلة]

* Types of LMI

1- cisco LMI
2- q933a LMI ⇒ Made by ITU (international Telecomm. union)
3- ANSI LMI ⇒ ANSI (American National standard I--)
4- dynamic (auto) LMI discovery ⇒ Made by cisco & it is the default for cisco devices

وهنا الروتر هيبعت LMI inquiry بالطريقة الاولى لمدة 6 مرات (دقيقة) ولو ال switch مردش ← الروتر ~ ~ ~ ~ ~ ~ الثانية ~ ~ ~ ~ ~ ~
~ ← الروتر ~ ~ ~ ~ ~ ~ الثالثة ~ ~ ~ ~ ~ ~ 6

بعيين الوحيد انك هتستنى 3 دقائق (Max) عشان تعرف ال LMI type

---

* The third step in FR operation

الروتر هيعمل خريطة لكل IP المقابل لل DLCI (اللي عرفها من step 2)

العملية دي بتتم من طريق IARP (Inverse ARP protocol)

السؤال هيبقى [ايه هو ال Next hop (IP) المقابله لل (PVC) DLCI ****]

↓
FR MAC

The configuration

(config)# int S0

(config-if)# incapsulation Frame-relay [ietf]

inc FR ← الكلا

option ↙ [ietf] ← لولم تكتبه هيبقى cisco by default

(config-if)# Frame-relay LMI-type {Cisco | ANSI | q933a}

→ لولم تكتب الامر ده ما Router cisco هيختار daynamic LMI discovery

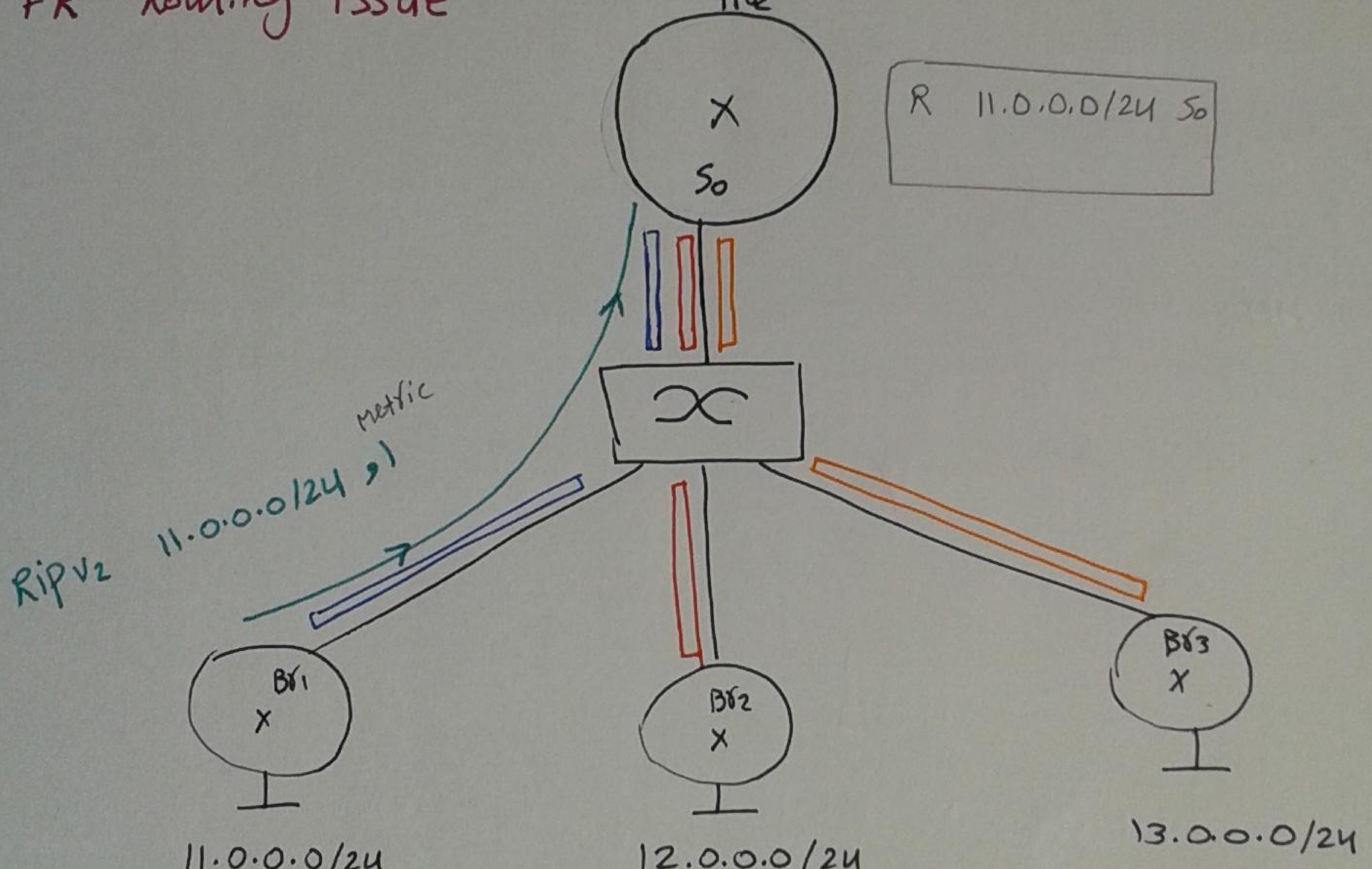
x (config-if)# Frame-relay MAP ip IP / 10.1.1.1 dlCI / 101

x (config-if)# Frame-relay MAP ip IP / 10.1.1.2 dlci / 102

} statically

لولم تكتب الامرين دول ما الروتر هيشتغل IARP ↓ Dynamically

FR Routing issue



المشكلة هنا ان لو Br1 بعت ال RTG Table بتاعه لل HQ ما ال HQ مش هيعرف يبعت الRTG Table بتاع Br1 لـ Br2 & Br3 عشان خاصية ال split horizon اللى بتقول لو اتعلمت حاجه من Interface معين ما هينفعش تخرج نفس الحاجه على نفس الـ Interface

وكان الحل هو ......

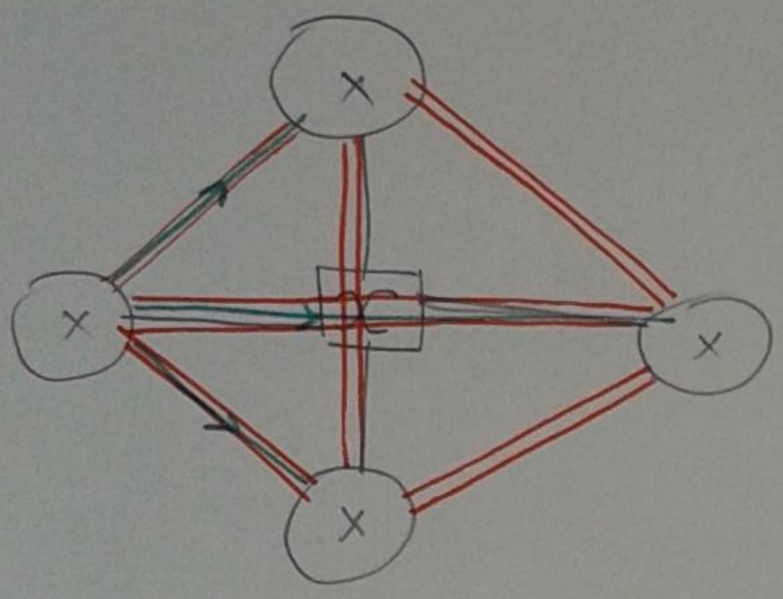
Solutions :-

[1] disable split horizon

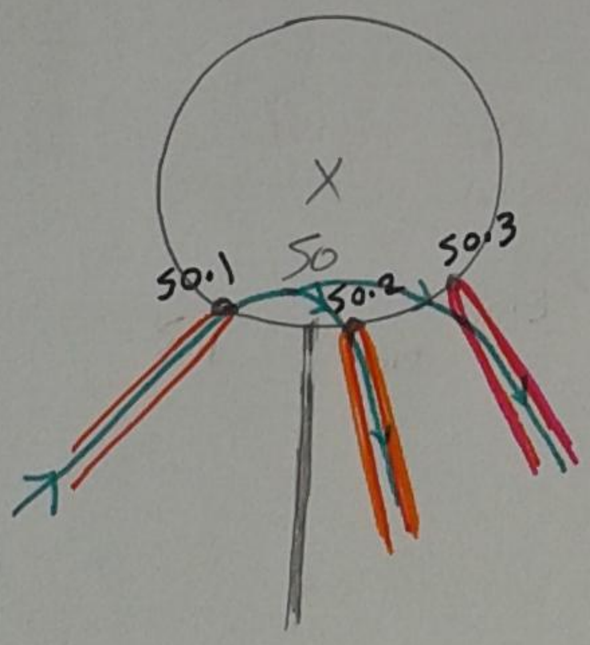
(config-if) # no ip split horizon ⟹ الشكله انك هتقع فى مشكلة الLoops

[2] use Static (مش هينفع لو الشبكه كبيره اوى)

[3] use Full Mesh topology ⟹ حرام عليك التكلفه والتعب



[4] Devide Main interface into point to point subinterfaces (99% of usage)



(config) # int S 0.1

(—subif) # ip add —— ——

Security

Security attacks

(1) Reconaissance attack

trying to discover network resources

- no of PCs
- no of switches
- no of routers
- servers
- services (Application)
- IP range
- MAC s

(2) Spoofing attack ≡ MASK querating

- IP spoofing
- MAC spoofing
- Router spoofing

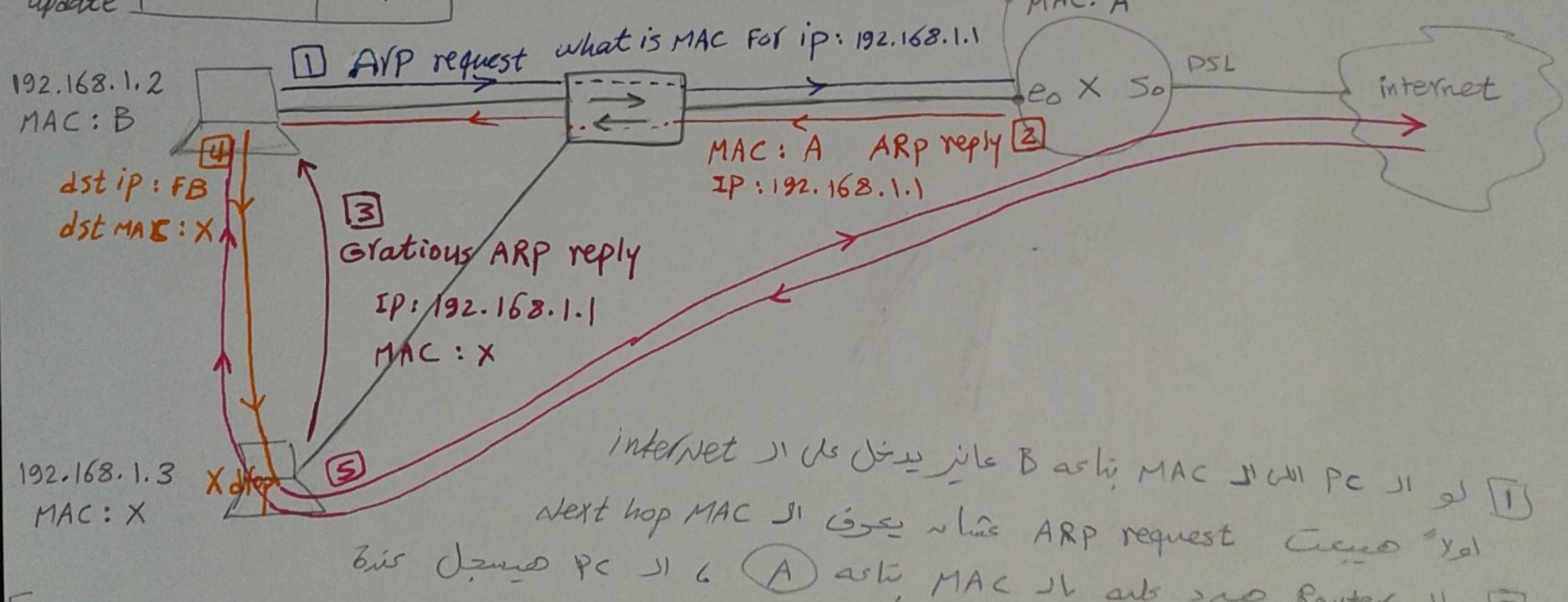
Spoofing ≡ sniffering ≡ earsdropping

ARP cashe

IP	MAC
~~192.168.1.1~~	~~A~~
192.168.1.1	X

latest update

Router spoofing



1 لو ال PC اللى ال MAC بتاعه B عايز يدخل على ال internet هيبعت ARP request عشان يعرف ال Next hop MAC اول حاجة

2 ال Router هيرد عليه بال MAC بتاعه (A) و ال PC هيسجل كدة في ال ARP cache ← ال MAC & IP [ملحوظة: تقدر تشوفها في ال DOS بالامر arp -a]

3 ال Hacker هيبعت Gratious Arp عشان يوهم ال PC انه هو ال Router وهيقوله Router IP فيه ال Router MAC = X

4 ولوقتي ال PC هيحذف ال latest update الاخير من ال ARP cache ويضع ال MAC = X اللى فيه ال

5 لو ال PC عايز يدخل على ال FB مثلاً ← يبعت طبعاً للجدول اللى كدة لازم يروح لل Default gateway اللى ال MAC بتاعه X وبالتالى لما ال Data تروح على ال Hacker و ال Hacker هيوقعها (drop)

5 معكد ال Hacker يكون اشرس ويتصنت على الداتا من انه يبعتها على ال Router
ولما الروتر يرد عليه هيبعت الرد على ال PC ، والحاله دى اسمها
(MAN in the Middle)

* عشان تعرف هل بيتم التصنت عليك ولا لأ ⇐ اعمل Tracert على ال DOS وهو
هيجيب لك ال Next hop IP ، لو ال Next hop IP هو ال Router بتاعك يبقى
تمام ، لو حد بيتصنت عليك هيجيبلك ال IP بتاع ال hacker مش الروتر

* عشان تمنع حد انه يغير لك ال MAC بتاع ال Gateway (Router) ممكن
تكتب ال MAC و ال IP بتاع ال Gateway بايدك static عن طريق الامر ده

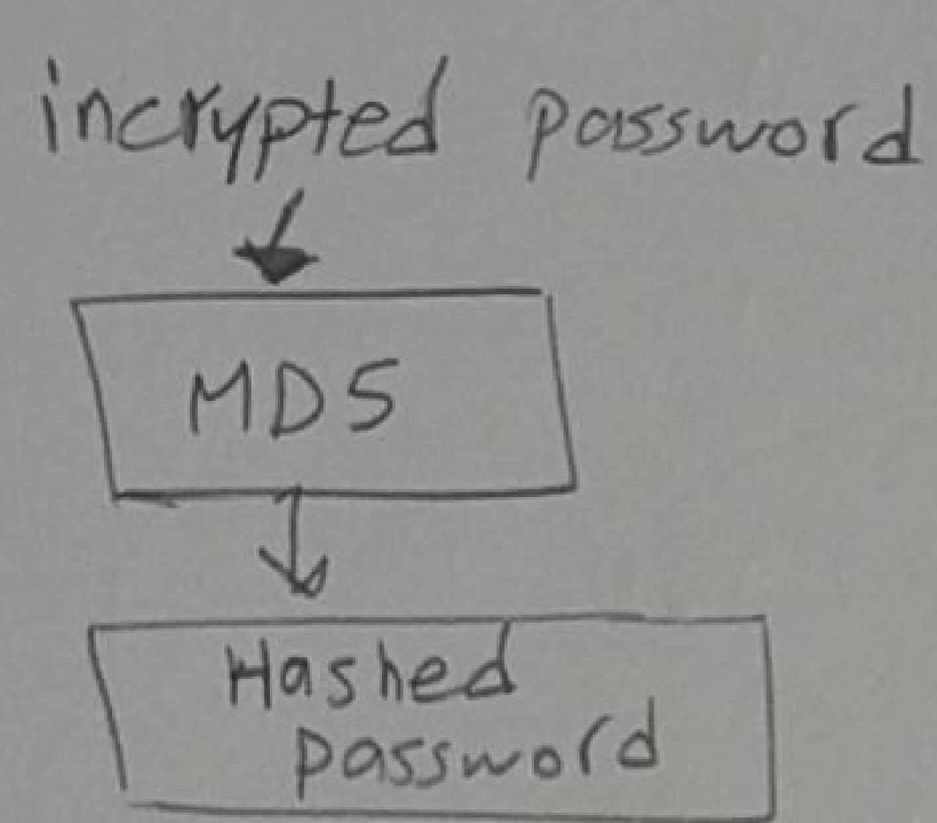
arp -s IP MAC

لكن عيبه انك لو عملت Restart لل PC هتضطر تكتبه تاني

3 Brut force attack

password guessing

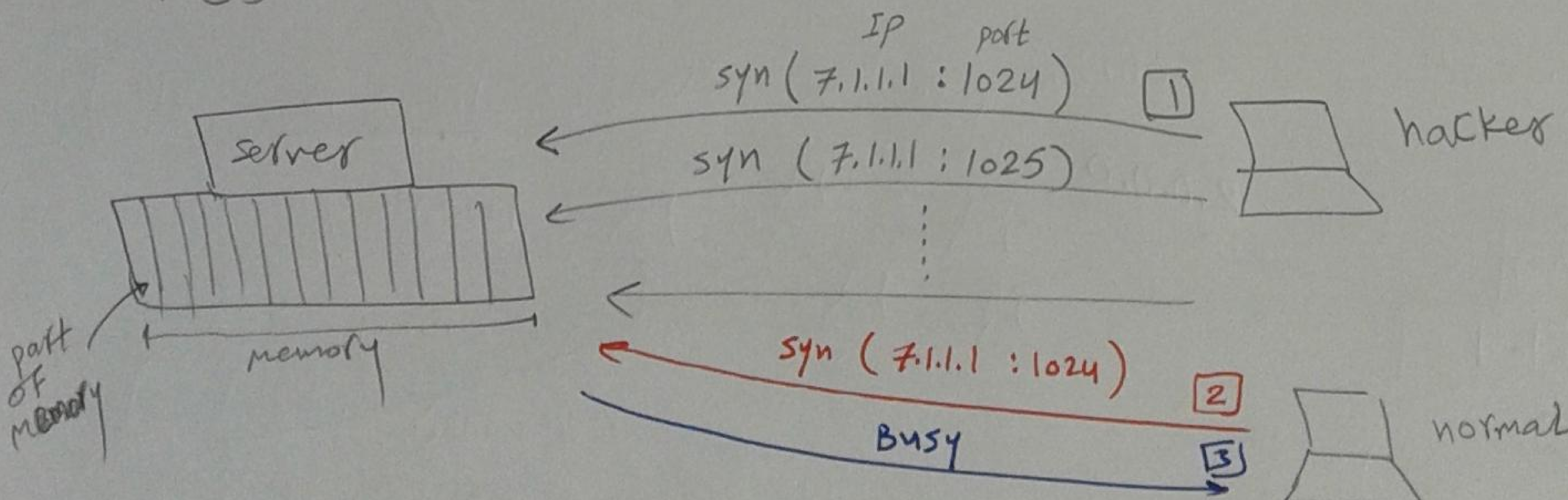
* هنا بيجرب passwords كتير اوى ويدخلها عند MD5 algorithm
لحد ما تطابق ال Hashed pass. وكده يبقى طلع ال password



Try ⇒ If error
Try new one and so on

4 DOS attack [Denial of service]

هنا عايز يوهم ال Server ان ناس كتير بتدخل عليه وانه مشغول طول الوقت ولو حد
عايز يدخل على ال Server ⇐ ال Server هيمنعه يدخل لأنه مشغول جداً



الطبيعى لما pc بيبعت فتح session جديدة مع ال server ، ال server هيحجزله جزء من ال Memory

[1] ال hacker هيبعت فتح sessions كتير جداً فى الثانيه الواحدة ، وكل session جديدة بتتفتح ، ال server بيحجزلها جزء memory ، هدف ال hacker هنا انه يشغل ال Memory كلها بتاعه ال server وبالتالى [2] لو جه pc عادى وعايز يفتح session جديدة مع ال server ⇐ [3] ال server هيرد عليه انه مشغول جداً . و مش هيفتح معاه اى session

⇐ الحل هنا ان الـ server ميقبلش يفتح اكتر من 5 sessions مثلاً لنفس ال pc فى الثانية

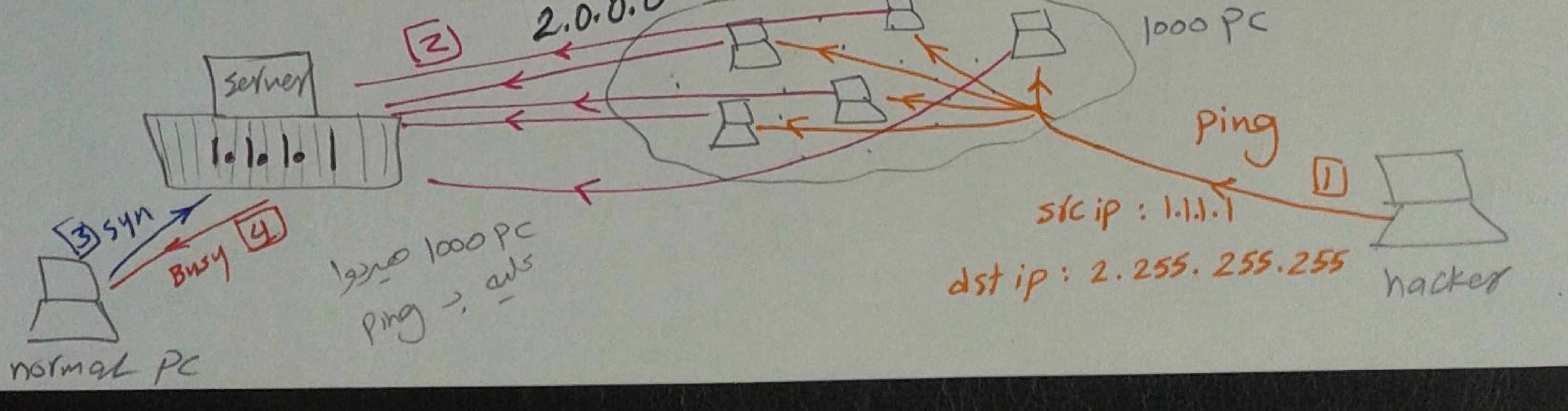
⇐ هل ال hackers هيسكتوا ؟؟؟ لأ طبعاً . دة اكل عيش !! عشان كدة هيفكروا فى الحل د ة ⇐

DDOS attack (Distributed DOS)

[1] ال haker هيروح على شبكه مثلاً فيها 1000 PCs وهيبعت لهم ping ب src ip بتاع ال server اللى هو فى حالتنا (1.0.1.0.1) على dst ip بتاع الشبكه 2.255.255.255 ولاحظ هنا انه بعت ل dst ip ⇐ Broadcast عشان يجبر كل ال PCs فى الشبكه 2.0.0.0 انهم يعملوا process

[2] ال 1000 PCs اول ماهيشوفوا ال ping ، كلهم هيعملوا process وهيردوا على ال server اللى ال Ip بتاعه (1.0.1.0.1) ب ping ، هنا بقى ال server ، كل pc هيعمل عليه ping هيحجزله جزء من ال Memory لحد ما الـ Memory كلها تتملى [3] ولو جه normal pc عايز يتكلم مع الـ server ، [4] ال server هيبعتلوا I'm Busy

[ال 1000 PCs فى الحالة دى اسمهم zombie يعنى الموتى الاحياء]



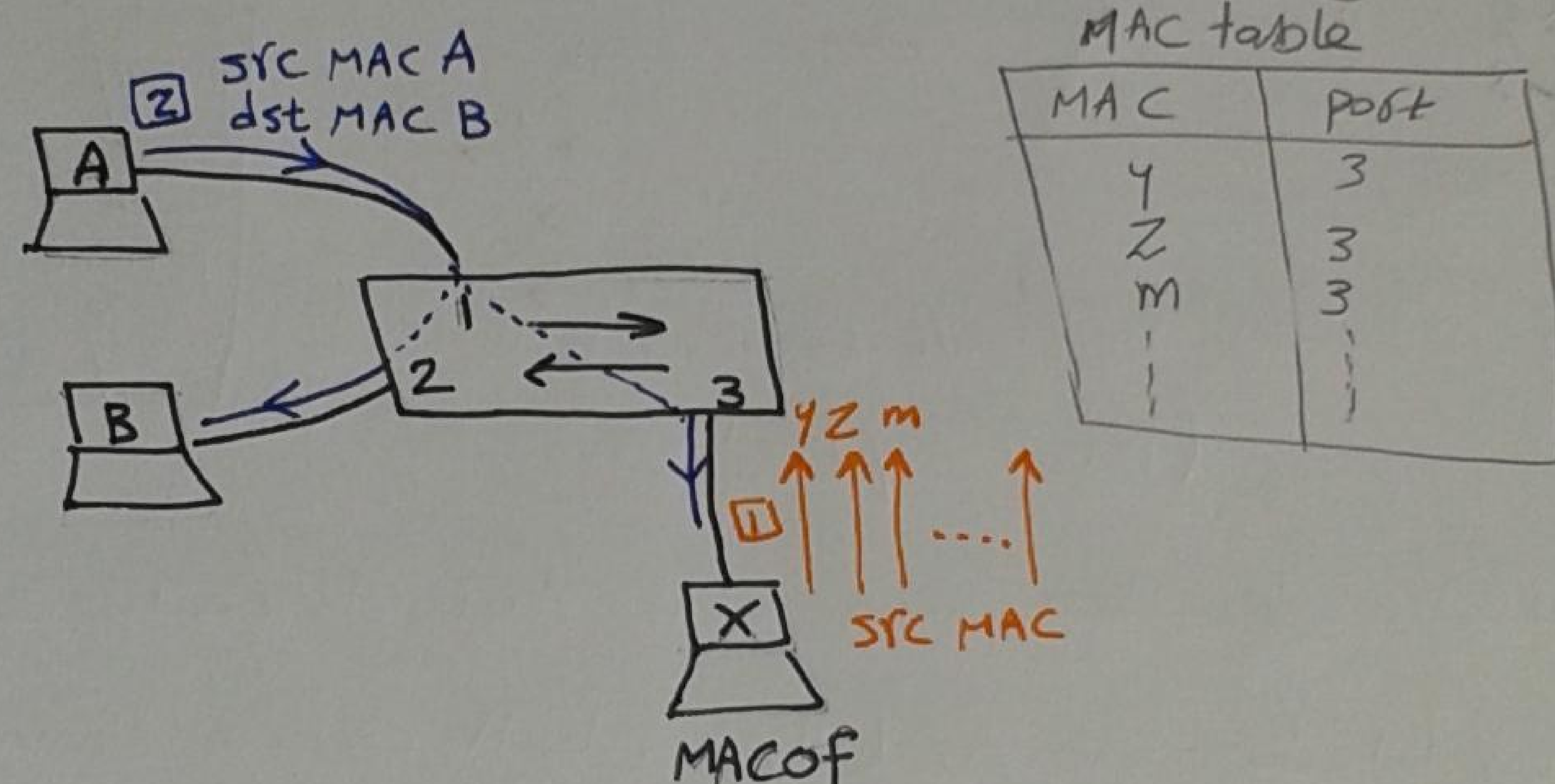
Security Mitigation مداواه الالام والجراح

1 switch security

تأصيل المشكلة

1 فى واحد اسمه MACOF عمل برنامج على اسمه ، اول ما ال switch هيفتح ، البرنامج ده هيبعت [src MAC Y ، src MAC Z ، src MAC .....] يعنى هيعلم ال switch ماكات كتير جداً [وهما مش موجودين اصلاً] ، كل اللى هيعمله ال switch انه كل ما هتجيله MAC جديده هيروح حفظه فى ال MAC table بتاعه لحد ما ال MAC table يتملى

2 لو جه PC حقيقى عايز يبعت حاجه لـ PC تانى ، اولاً لازم يعدّى على ال switch ، ال switch هياخد ال dst MAC وهيقارنه بالجدول اللى عنده ، مش هيلاقيه موجود فى الجدول فيهيضطر انه يـ Flood ، هيجى ال Hacker هياخد ال Data اللى جايه من ال Flooding وهيتصنت عليها [هنا ال Swich بقى عامل زى ال Hub]



MAC table

MAC	port
Y	3
Z	3
m	3
⋮	⋮

switch port security

(config)# interface fast Ethernet 0/3
(config-if)# switch port port-security

معناه → ① only one MAC allowed to access
→ in case of Violation (تعدّى) ⇒ port will shutdown by default
(shutdown ← هتتقفل فى وش الكل)

option

(config-if)# swith port port-security Maximum 5 → لو عايز تحدد اكبر عدد من الناس اللى مسموح لها تدخل على الport دى، ولو 6 مثلاً دخلوا على الport ← ال port هتتعطل shutdown by default

(config-if)# switch port port-security MAC MACA
(--)# ~ ~ ~ ~ MAC MACB
] → لو عايز تسمح لـ PCs محددة تدخل على ال port دى ولو PC له MAC Y مثلاً دخل على ال port ← ~ ~ ~ ~ ~ ~

ممكن متكتبش الامرين دول وتكتب الامر ده

(config if)# switch port port security sticky

(config-if)#switchport port security violation {restrict | protect}

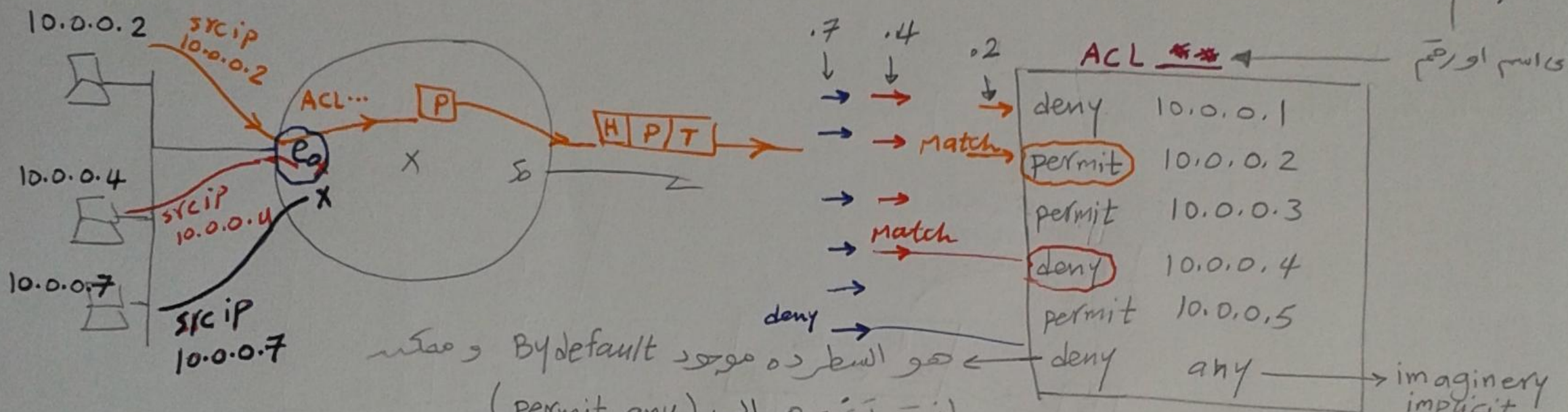
الامر دة بتكتبه لو فى حاله التعدّى او الاختراق مش عايز الـ port تقفل (shutdown)

permit → normal فى وش كل الناس ، تكمل عايز تقفلتر الناس بمعنى
deny → hacker

← لو لم تكتب الامر دة هيبقى الـ default هو (لو فى حاله اى تعدى) ←
Shutdown

Router security

ACL [Access control list] → ع وب security ← اللى معروفش معدّهوش



ای اسم او رقم

هو السطر ده موجود ByDefault وممكن انت تغيره الى (permit any)

الترتيب مهم اوى وانت بتكتب الـ ACL عشان بيمشى سطر سطر ولو لقى الـ Ip اللى داخل مطابق لسطر معين مكتوب بالفعل فى الـ ACL ← هينفذ اما access او Deny على حسب المكتوب فى السطر اللى فيه الـ Ip ، ولو ملقاش الـ Ip فى الـ ACL هينفذ الـ Default اللى هو (deny any) الا فى حاله انك كاتب اخر سطر (permit any)

* ملحوظه قبل ما تكتب الـ ACL لازم تعرفها الاول على اىّ Interface (فى حالتنا Eo)

ACL Types

- Ip standard ACL
  - old → numbers (1 - 99) (1300 - 1999)
  - new → name (any name)
- Ip Extended ACL
  - old → numbers (100 - 199) (2000 - 2699)
  - new → name (any name)

(1)* Ip Standard ACL

it filters data based on src ip only

[A] create ACL

numbered :

لازم تكتب واحد مابين الاقواس { }

option

(config) # access list 1-99 { permit | deny } src ip [wild card Mask]

or

① ال wild card MASK دة option وهو عبارة عن (0000...1111) 32bit ⇐

لو ال bit = 0 يعني عايز ال bit القابله له في ال IP بالتحديد

لو ال bit=1 يعني X (don't care)

لو مكتبتش ال wild card MASK في ال Command ⇐ هيبقى ال Default اللي هو 0.0.0.0

يعني انا عايز ال IP دة بالتحديد

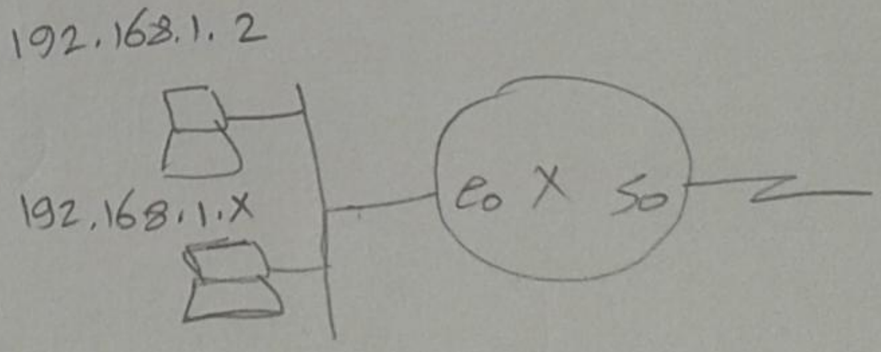
(EX1) (config) # access list 7 permit 192.168.1.10

معناه ان عايز ال IP دة (192.168.1.10) بالتحديد يبقى permit

(EX2) (config) # access list 7 deny 192.168.1.0 0.0.0.255

معناه ان عايز الـ IPs دول (192.168.1.X) اللي هما (192.168.1.0 ↔ 255) كلهم deny

ملحوظة / ترتيب السطور مهم جداً في ال access list فمثلاً



(config) # access list 7 deny 192.168.1.2

(config) # accesslist 7 permit 192.168.1.0 0.0.0.255

* بالامرين دول هو لو جاله (192.168.1.2) هيشوف السطر الاول و هيمنعه من الaccess

* تكمن لو غيرت ترتيب السطرين ف الحاله دى اول ما هيجيله (192.168.1.2)

هيشوف السطر الاول (192.168.1.X) فيعديه و يبدء السطر التانى مش هيكون

ليه اى لازمه

named :-

(config) # ip access-list standard name

(config-std-nacl) # {permit | deny} src ip [wild card mask]

std ← standard
nacl ← name ACL

* لاحظ انك كتبت فى الامر الاول (IP & standard) حشان تعرّف الـ Router النوع (standard او Extended) لكن فى الارقام فهو بيكونه عارف صه الرقم

* الميزه هنا انك بتكتب اسم الـ access list مره واحده بس وبعدين بتكتب كل الـ IPs مره واحده ، على عكس الـ numbered ، كمان لازم تكتب اسم الـ access list مع كل IP حاجز تعرفه او كل مجموعه IPs مع بعض

* وكمان من ميزة انك لو عاوز تمسح سطر هتمسح السطر لوحده على عكس الـ Numbered ACL ← لو كتبت (no access-list 7 ----) (config) # ← هيمسح الـ ACL 7 كلها

حشان تشوف الـ (create ACL) بتكتب الـ command دى [# sh access-list]

B) activate access control list (ACL)

(config-if) # ip access list-group number or name {in | out}

in ← while receiving (before routing)
out ← while sending (after routing)

حشان تشوف الـ interfaces بتكتب الـ command [# sh ip int]

اهم الـ shows اللى ممكن تلزمنا

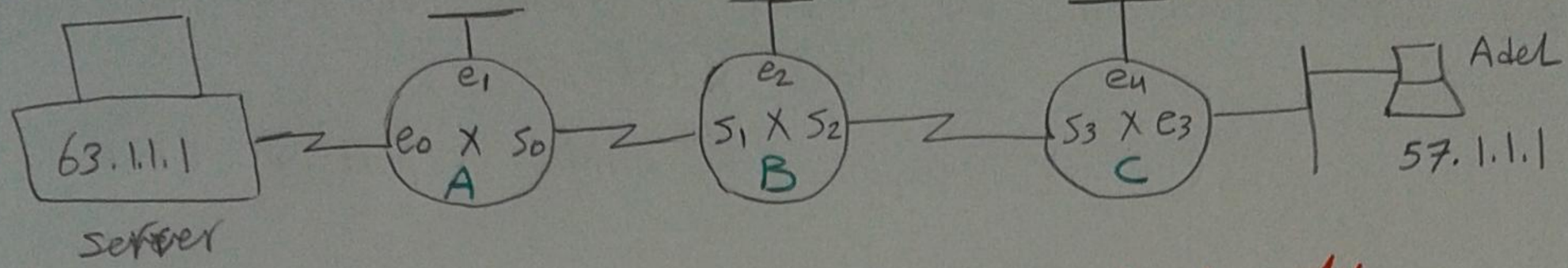
intro : # sh run
sh ip int brief

Routing : # sh ip route
sh ip protocol

Switching : # sh VLAN
sh int trunk

security : # sh access-list
sh ip int

EX



restrict adel only from access to server subnet only

create

A(config)# ip access-list standard Adel

A(config-std-nacl)# deny 57.1.1.1 [0.0.0.0] ← option
WCM

A(config-std-nacl)# permit any or 0.0.0.0 255.255.255.255
wild control mask

activate

A(config)# int e0

A(config-if)#ip access-group Adel out

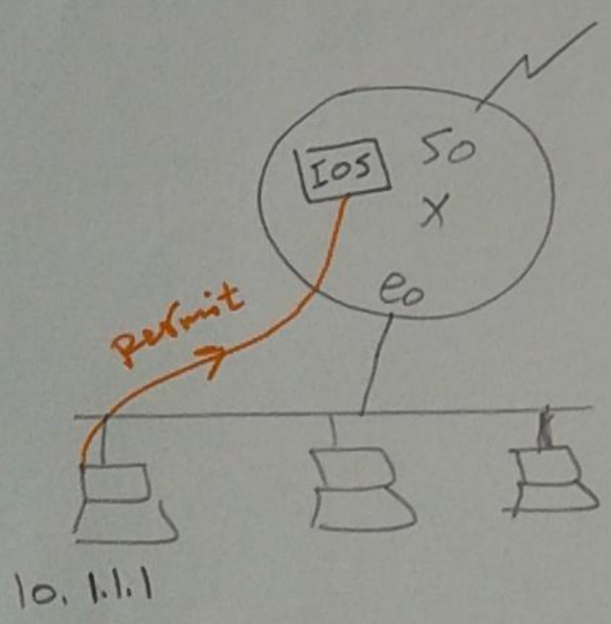
← بمعنى ← نفذّي ال ACL اللي اسمه Adel والداتا خارجه من عندك

Rule 1 : access should contain at least 1 permit

Rule 2 : Standard ACL should be placed as close as possible to distination

عشان منخنّش على ال src

EX



(config)# access-list 3 permit 10.1.1.1

((config)# line VTY 0 4

(config-line)# access-class 3 in → ???

لازم نحدد

② IP Extended ACL

it filters data based on 1- Tcp/IP protocol (L3 & L4 protocol)
2- src IP & dst IP
(option) 3 - application name or port no (L7)

[A] Create ACL

numbered ACL :-

(config)# access-list 100-199 {permit/deny} Tcp/IP protocol src ip W.C.M

dst ip W.C.M [eq Application name|port no]

note

① Tcp/IP protocol → is L3 & L4 protocols as TCP & UDP & ICMP & Eigrp & .....
* If you write (IP), it means any protocol

② W.C.M must be written ⇒ it is not option here but it was option in IP standard ACL

③ [eq Application name | port no] is option, If you don't write it
→ the default will be any

Ex of Application name | port no

FTP	20, 21
SSH	22
Telnet	23
SMTP	25
HTTP	80
HTTPS	443

named ACL :-

(config)# ip access-list extended name

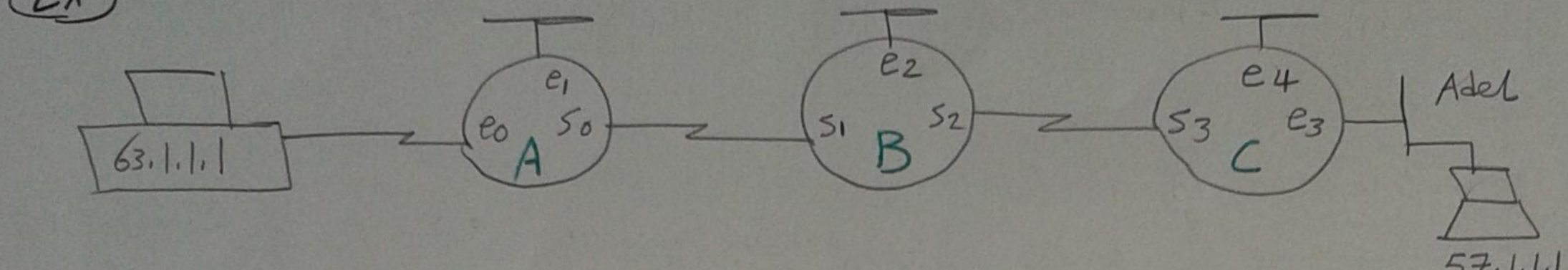
(config-ext-nacl)# {permit/deny} Tcp/IP protocol src ip W.C.M

dst ip W.C.M [eq Application name|port no]

[B] Activate AcL :-

(config-if) # ip access-group # or name {in | out}

Ex



restrict 57.1.1.1 (Adel) only From browsing only on server only

Create (TCP) اللي هو تبع HTTP تبع Browsing حشان ال

C (config) # access-list 199 deny Tcp 57.1.1.1 0.0.0.0 63.1.1.1 0.0.0.0

eq ~~HTTP~~ WWW

HTTPS & HTTP كمان عشان متعت

C(Config) # access-list 199 permit IP any any

activate

C (config) # int e3

C (config-if) # ip access-group 199 in

Rule 3 : Extended ACL should be placed as close as possible to src

عشان تفلتر ال ip من الاول خالص عشان ميعملش processing كتير

مع العلم في الحاله دي (Extended) انت اصلا محدد ال dst IP & src IP وبالتالي لو وضعتوها على اي interface (e0, S0, S1, S2, S3, e3) مش هتفرق

لكن من الافضل انك تفلتر من على طول وميعملش processing كتير

Note / this command 57.1.1.1 0.0.0.0 (src ip, wcm) can be shorted to host 57.1.1.1

and also 63.1.1.1 0.0.0.0 (dst ip, wcm) host 63.1.1.1

Security Mitigation (continone)

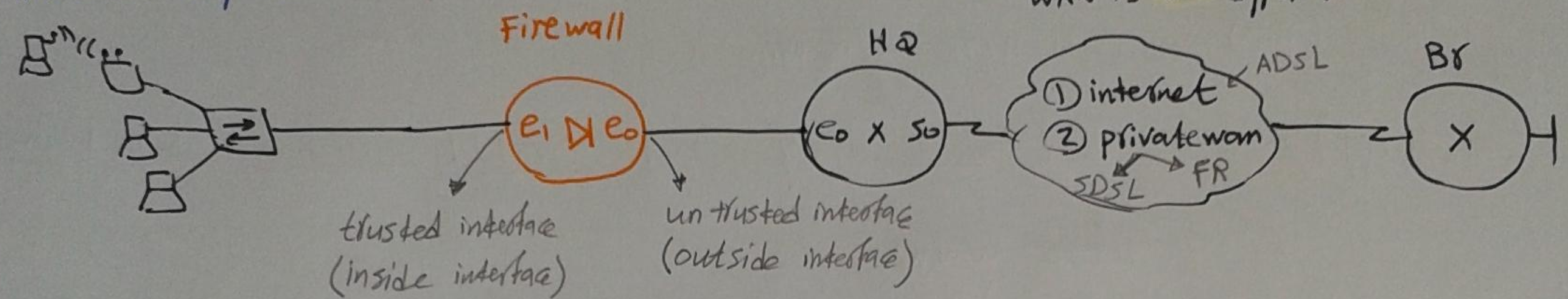
1. switch security
2. Router security

---

3. Firewall ملحوظة / كل ال Interfaces اللى على ال Firewall نوعها Ethernet

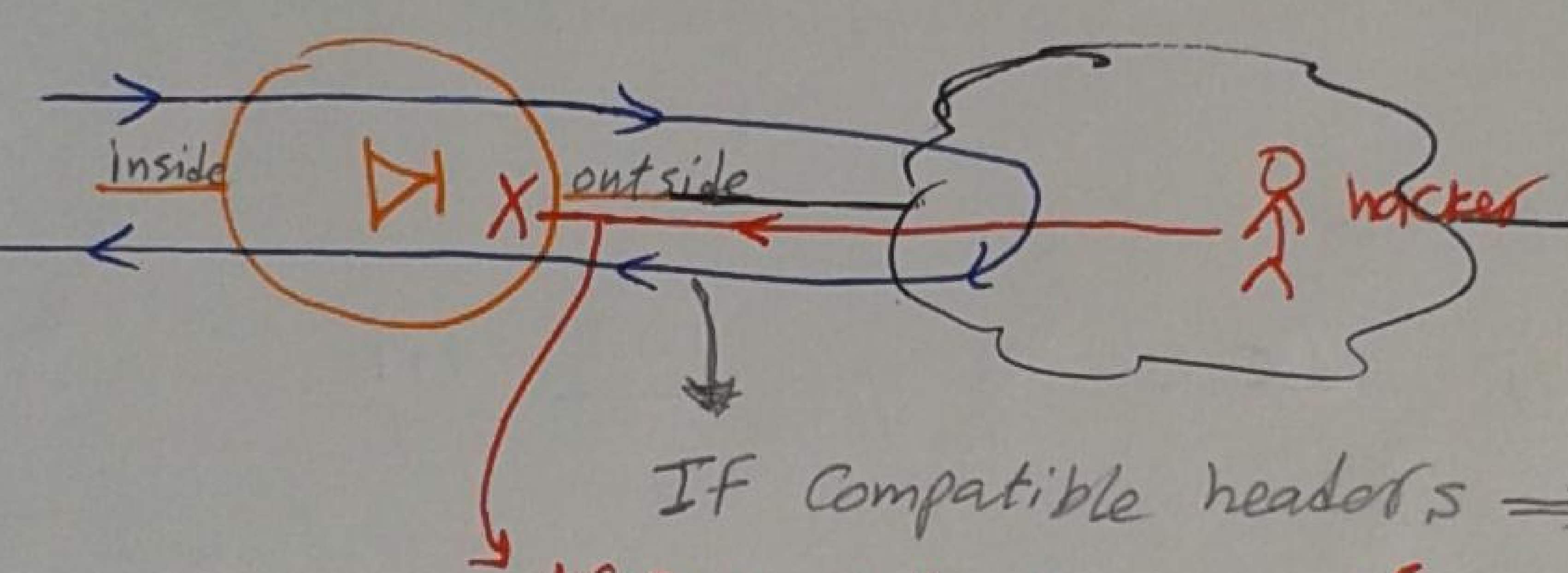
Firewall operation

1. Data from inside allowed to go outside by default
2. Data from outside is not allowed to go inside unless it is a reply for internal request



inspection table

L3 & L4 headers src ip , dst ip TOS , TTL , protocol , src port , dst port , squ # , ACK , -----



IF compatible headers ⇒ permit to enter

drop packets because of non compatible headers

ال firewall فيه inspection table اللى موجود فيه (L3 & L4 headers) من ال Frames اللى خارجه منه

← اى packet داخله من outside ⇐ ال Firewall بيشوف ال L3 & L4 headers و هيطابقهم باللى عنده فى ال inspection table ، لو compatible headers هيسمح لل packet بالدخول فقط

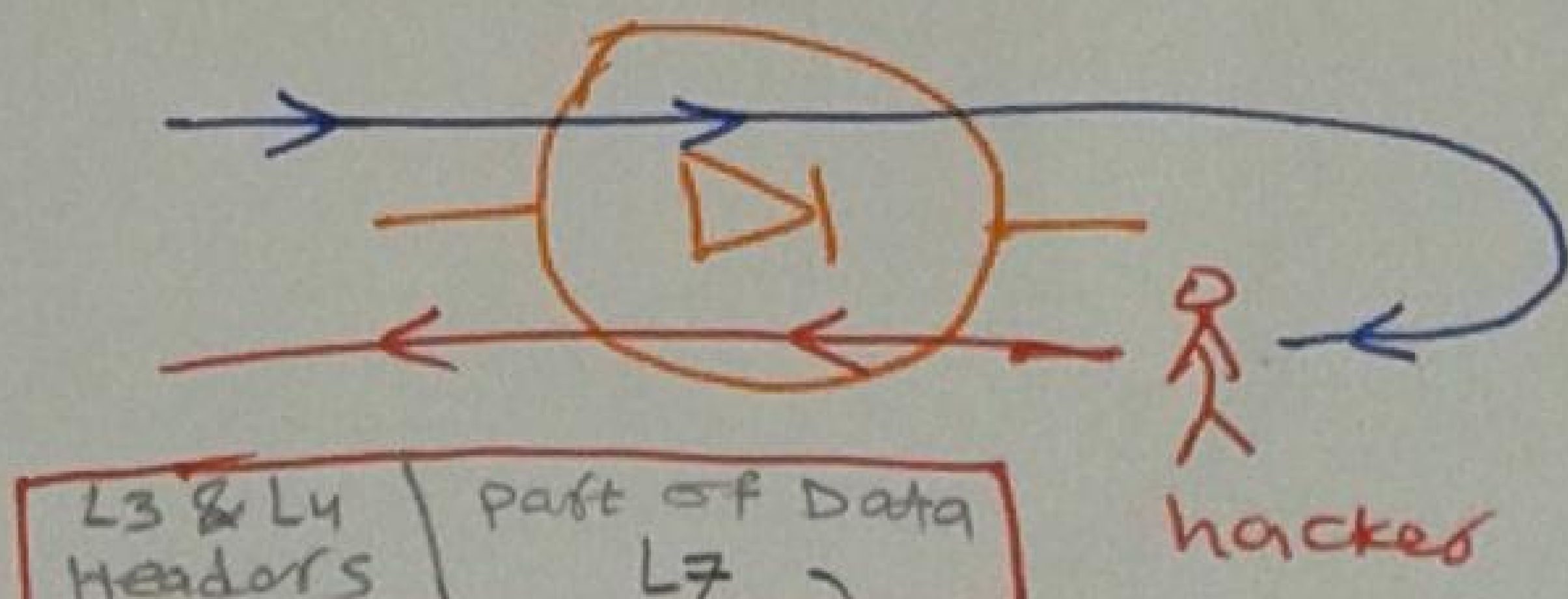
ولكن موجود bug ، وهى انه ال hacker يقدر ياخد اى packet راجعه ويسيب ال headers زى ماهى بس يغير فى ال Data نفسها ويحط virus مثلا ساعتها ال Firewall هيسمحلها تدخل مادام ال L4&L3 protocols compatible

حل المشكله دى ⇐ فى انه Cisco عملت

PIX Firewall (Application wirefall)

(deep inspection)

L7 inspection



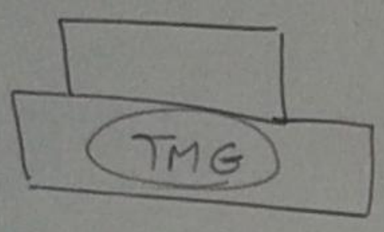
Malicious File

مؤذى

PIX Firewall

Application Firewall
(deep inspection (L7))

Software ↓ ISA by Microsoft
بعد التطوير ↓ TMG
(Thread Management Gateway)



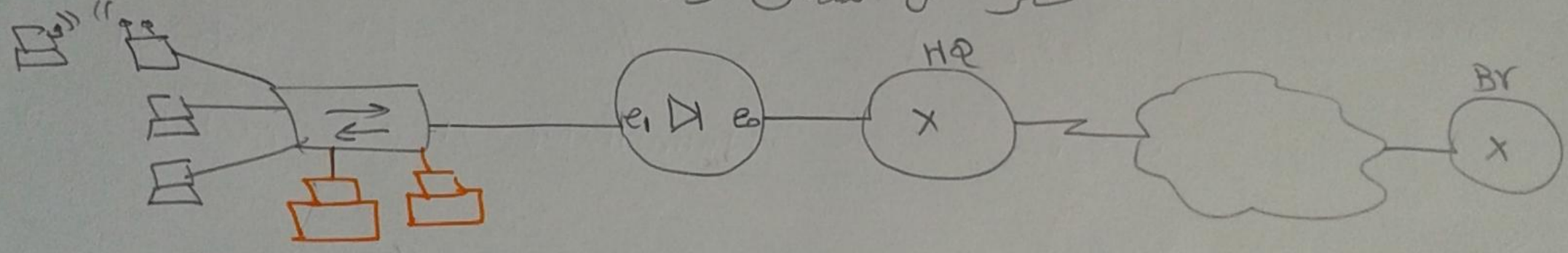
هتسطب البرنامج على pc

رخيص بس عيبه انه بطئ اوى عشانه ال S/W كتير طلع فيه bugs

Hardware ↓ ASA by cisco H/W
(adaptive security Appliance)

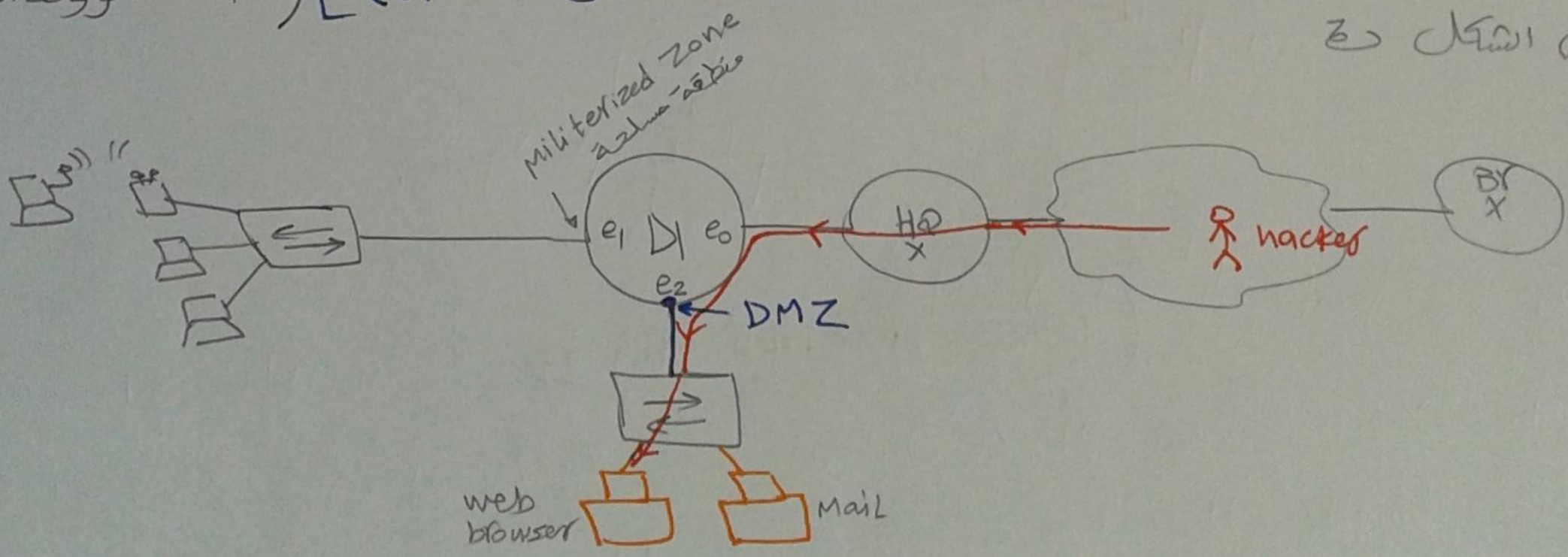
سريع جدا عشانه H/W بس غالى اوى

لو انت عندك servers فى ال LAN اللى فى ال HQ وعايز ناس من اللى موجودين فى ال BR يدخلوا على ال servers دى ← كده انت هتضطر تفتح ثغرة فى ال firewall لكده ده خطر فى الشكل دة



الحل للمشكلة دى انك هتشترى Firewall له رجول جديدة غير (inside&outside) والرجول دى اسمها [De-Militerized zone (DMZ)] (منطقة منزوعة السلاح)

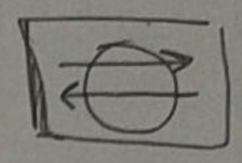
فى الشكل دة



وبالتالى لو ال Haker عايز يدخل على ال LAN بتاعتك ← هيقدر يعبر من ال firewall اكس ١ عن طريق ال (DMZ) interface

بكبه مازل هناك خطر ← انا بالفعل اقدرت احمي ال LAN من ال haker
بكبه ما زال ال servers معرضه للخطر ويقدر ال hacker يدخل يخرّب فيهم
← عشانه كده كانه الحل في IDS

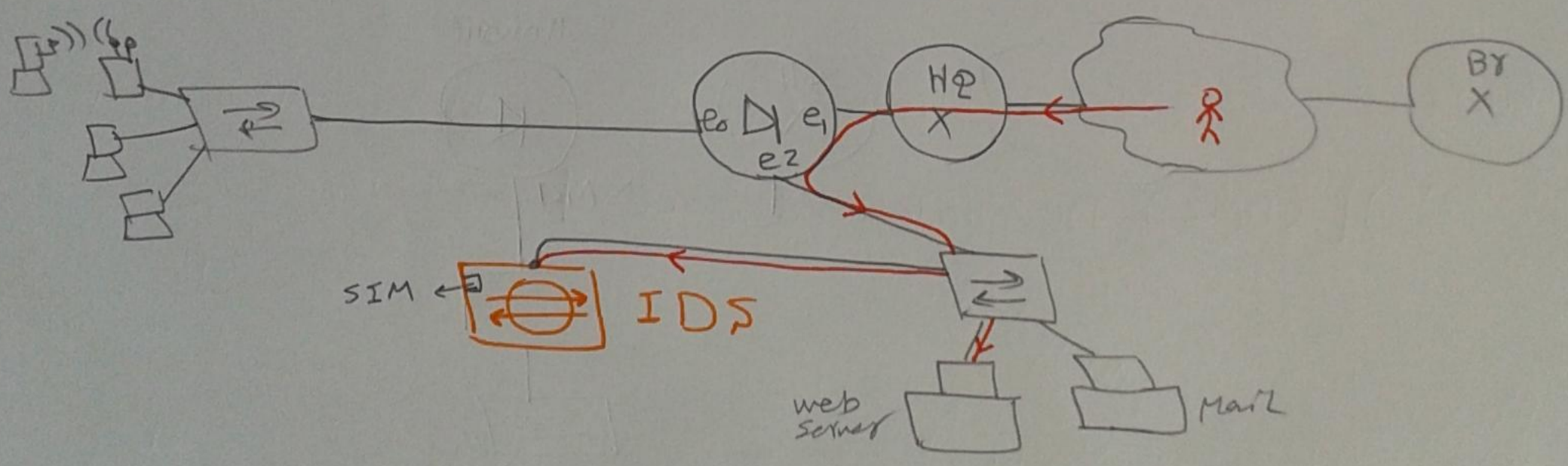
3] IDS (Intrusion Detection system) ⇒ وهزه



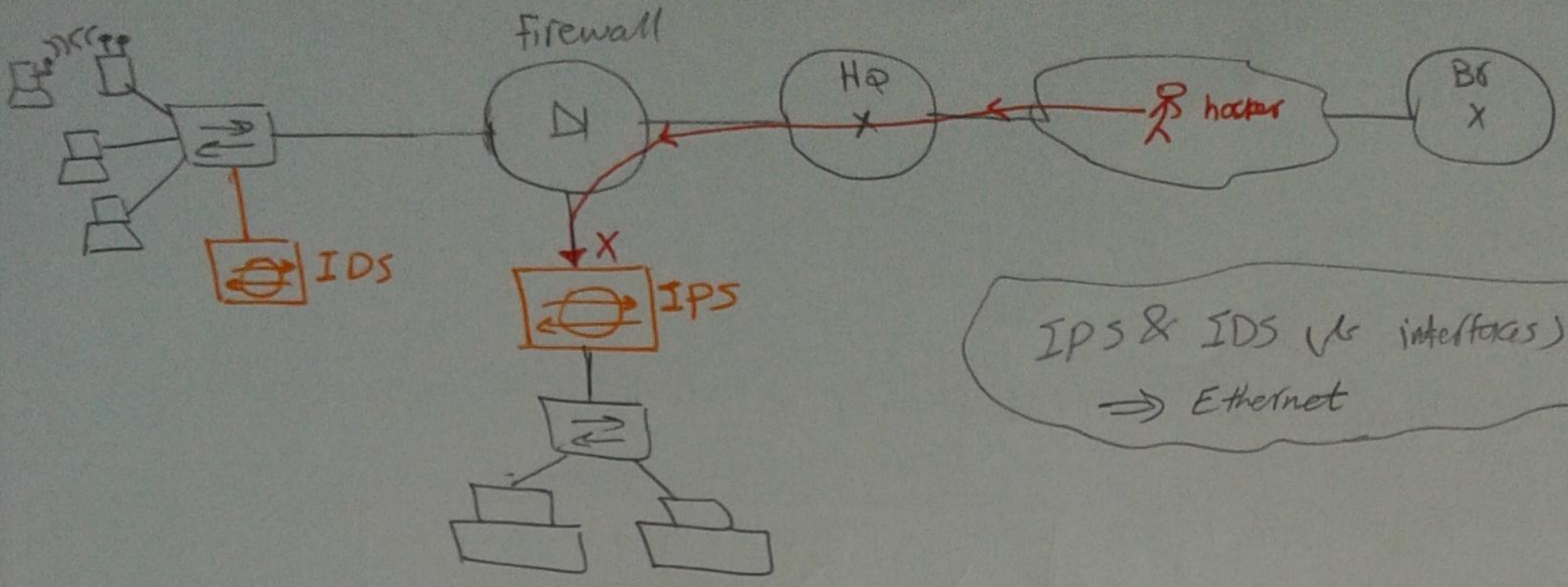
IDS operation

- IDS compares data to attacks signature file
→ If no attack → no response
→ If attack → send alarm to adminstrator

ودة عبارة عن Sensor او Detector فقط
كل اللي بيعمله انه عنده File اسمه (attak signature file) ودة بيبقى فيه
كل انواع ال (attakes) اللي تم اختراعها من قبل (all known attacks)
* كل packet بتدخل عليه ← بيدخل على ال Data ويقارن ال Data دي بال attacks اللي عنده
← لو ال Data مطلعتش attack هيسمح لها بالدخول
← ~ ال Data طلعت attack ← هيرسل alarm او SMS message
لـ Mobile بتاع ال Adminstrator وهو يتصرف



لكنه اخترعوا ال IPS (intrusion prevention sys.) ودة افضل من IDS
عشانه بيقدر يمنع ال attack من الدخول على ال servers اصلاً + انه
يقوم بنفس عمل ال IDS فانه بيبعت رساله لل admin.
وكبرة كانه من الافضل انك استخدم ال IDS داخل ال LAN عشانه اعرف
من خلاله محاولات الاختراق داخل ال LAN و اجهزة الموظفين



IPS & IDS لـ interfaces الـ كل / بـ X
⇒ Ethernet

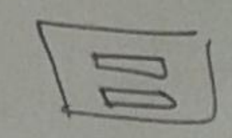
IPS operation

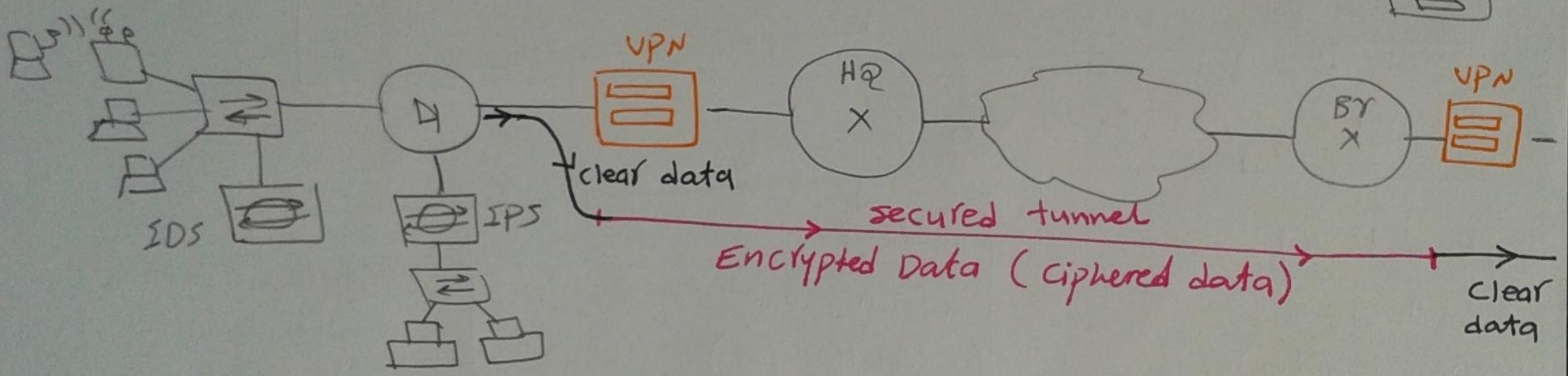
- IPS compares data to attacks signature file

→ If no attack → forword data

→ If attak → stop attak & send alarm to adminstrator

4 VPN appliana : (vertual private network appliana) هو

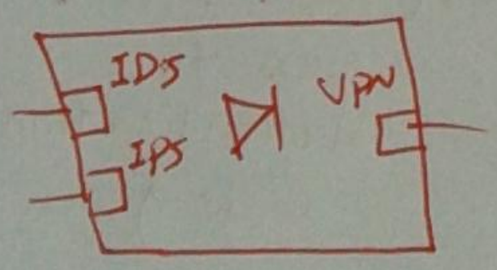




note

ASA Firewall is made by cisco

it has as buit in all these devices (VPN, IPS, IDS)



ASA firewall

① VPN devices

1. VPN appliance
2. ASA
3. Router

② VPN protocols

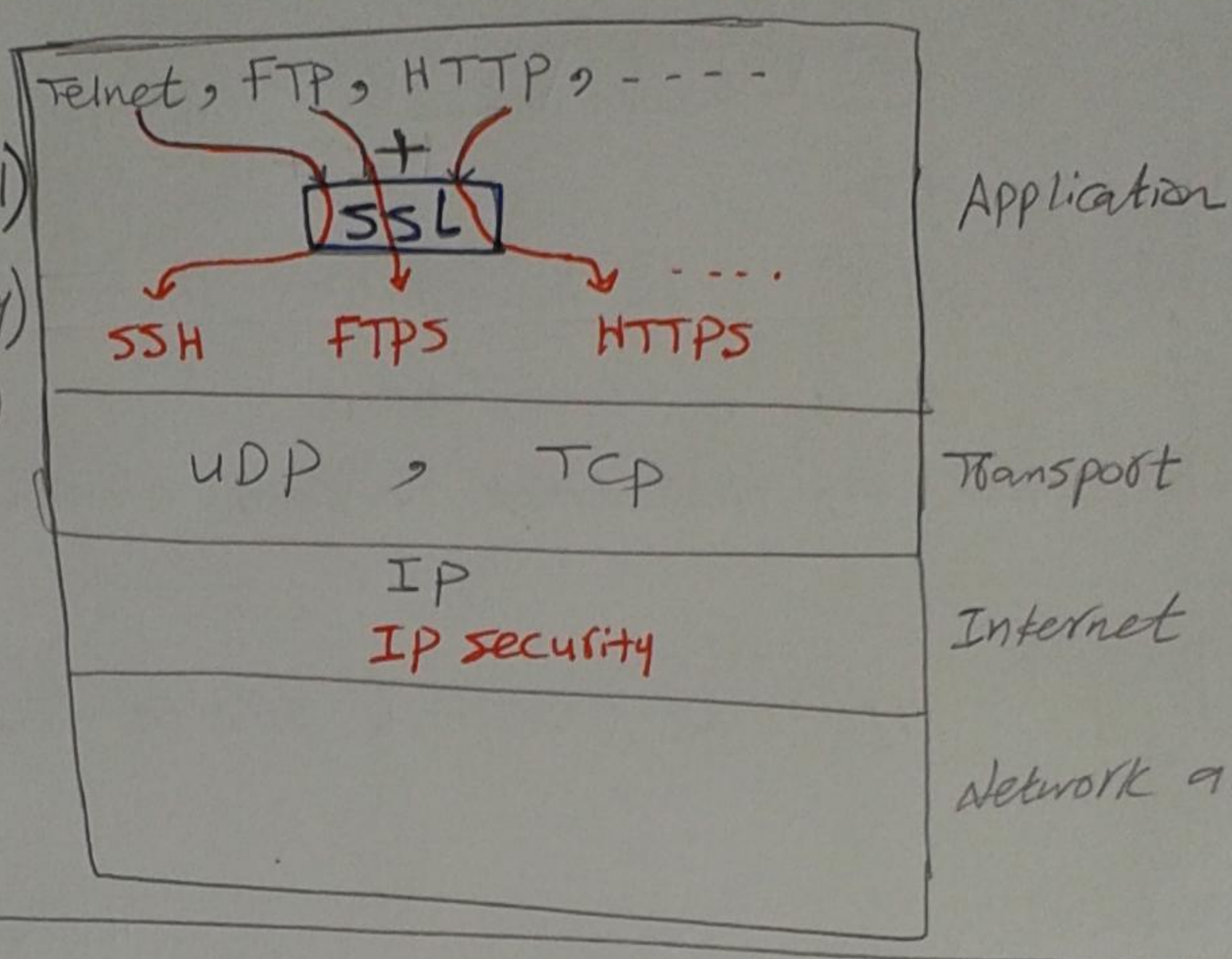
protocols that do confedentiality & Integrety & Authentication

SSL : secure socket layer

Telnet + SSL → SSH (secure shell)

FTP + SSL → FTPS (FTP security)

HTTP + SSL → HTTP (HTTP security)



* IPsecurity is ~~more~~ stronger

③ VPN operation (C, I, A)

Confedentiality
سرية المعلومة
(data Encryption)

→ symetric Encryption key
(Encrpted key = decr. key)

EX1 : DES : Data Encry. Standard
EX2 : 3DES : 3rd ~ ~ ~
EX3 : AES : Advanced Encry. Standard
EX1 اقوى من EX2 اقوى من EX3

→ Asymetric Encryption key
(Enc. key ≠ decry. key)

EX1 : RSA : rivest shmir adel man
EX2 : ELGAmal

EX1 اقوى من EX2

Integrity
سلامة المعلومة
(data Hashing)
(digital signature)

HMAC -MD5 (128 bit)
HMAC -SHA (156 bit)

HMAC : (Hash Based Message Authentication Code)

كل packet بيبعت مع 128 bit كاوتغراف

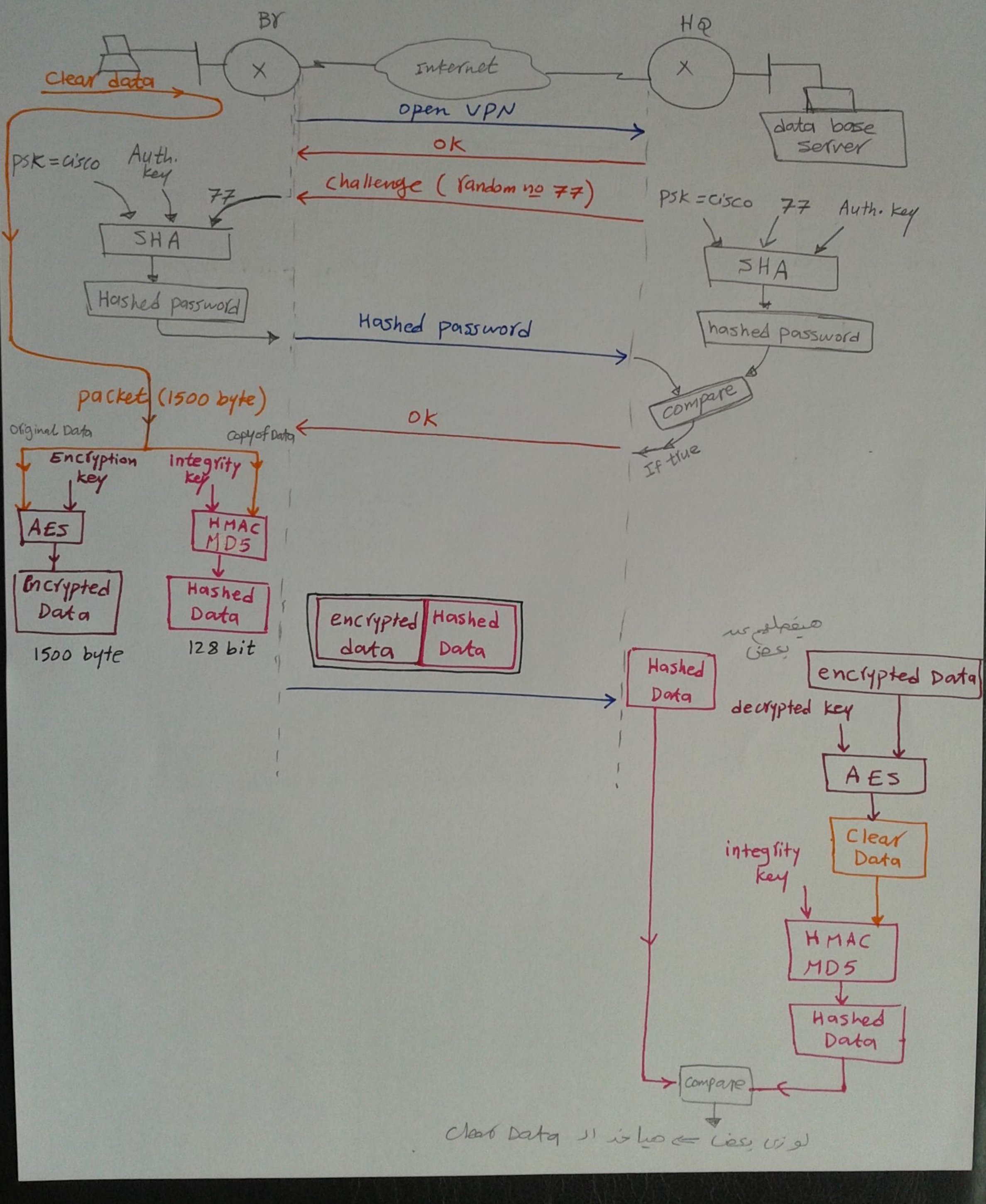
Authentication
التأكد من مصدر المعلومة
(password hashing)

MD5
(Message digester v.5)
50 day بكسر الـ pass باكتة بعد

→ SHA
(secure Hashed algorithm)
برامج التشويه الاعلى
الـ hacker يقدر يكسر الـ password
50 month باكتة بعد
(قوى جدا)

note/ PSK is (pre-shared key), it is a password that ~~is~~ well-known
In both server in HQ and PC in BR

العملية دى بطيئة جدا لكن جعلت ال security فى منتهى القوة

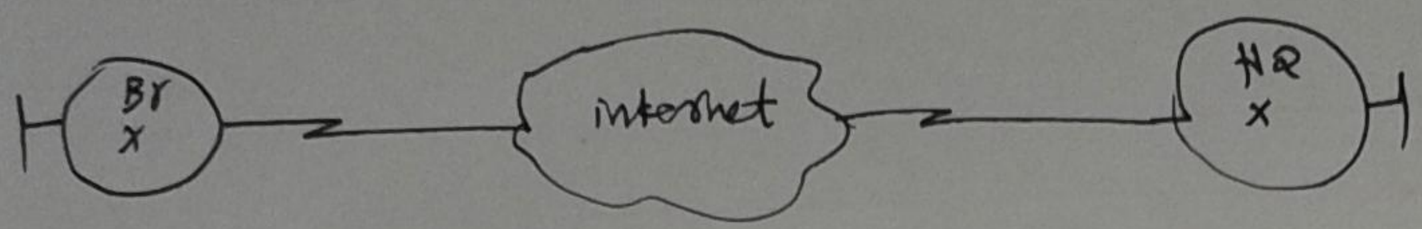


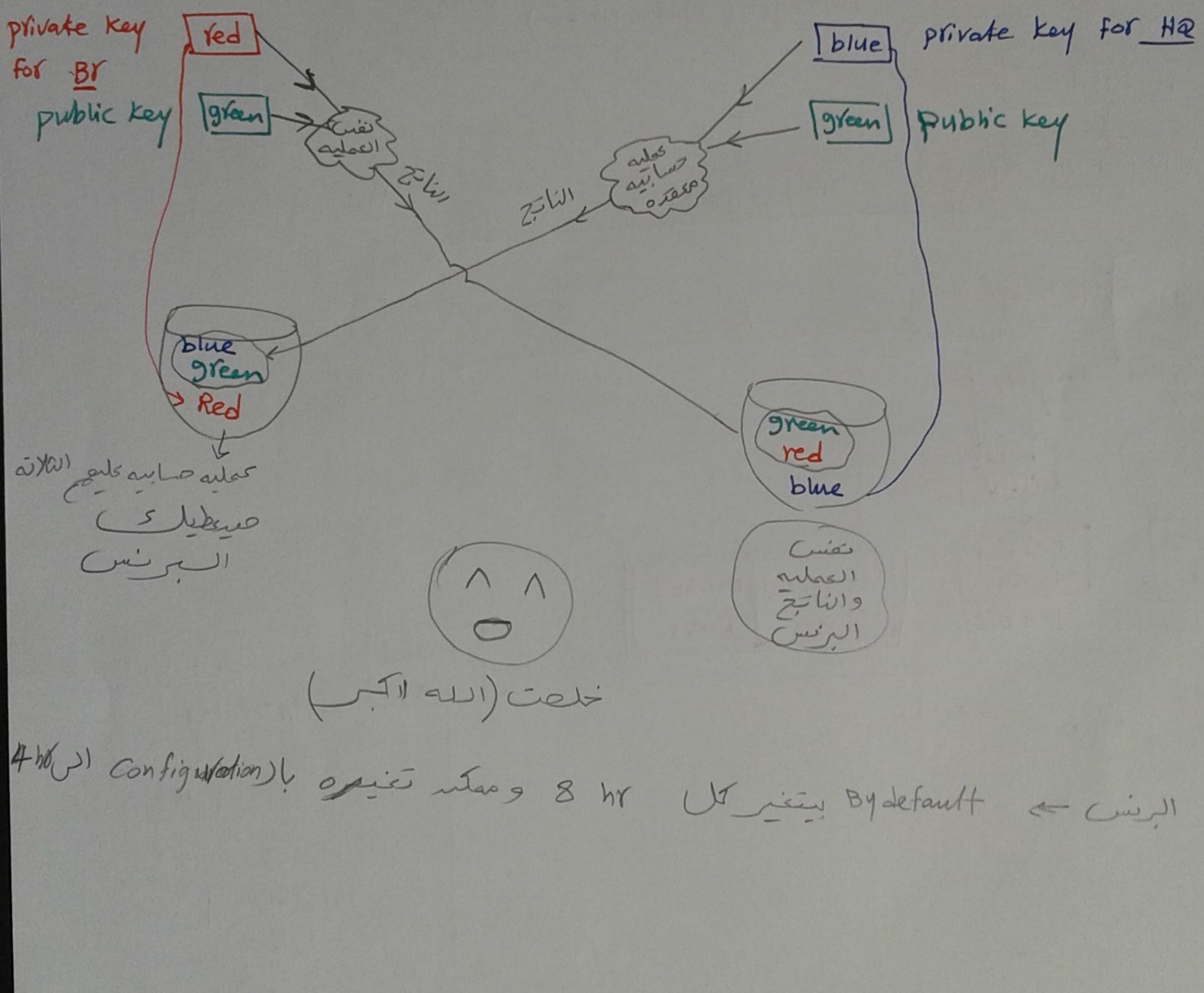
ناقص اخر حاجه وهو ان اعرف ازاى بكوّن الـ Keys Encryption & Auth. & integrity

Encryption key = Authintication key = integrity key = البرنس ⇐ من الواقع

IKE [internet key Exchange)

by Diffie - Hellman

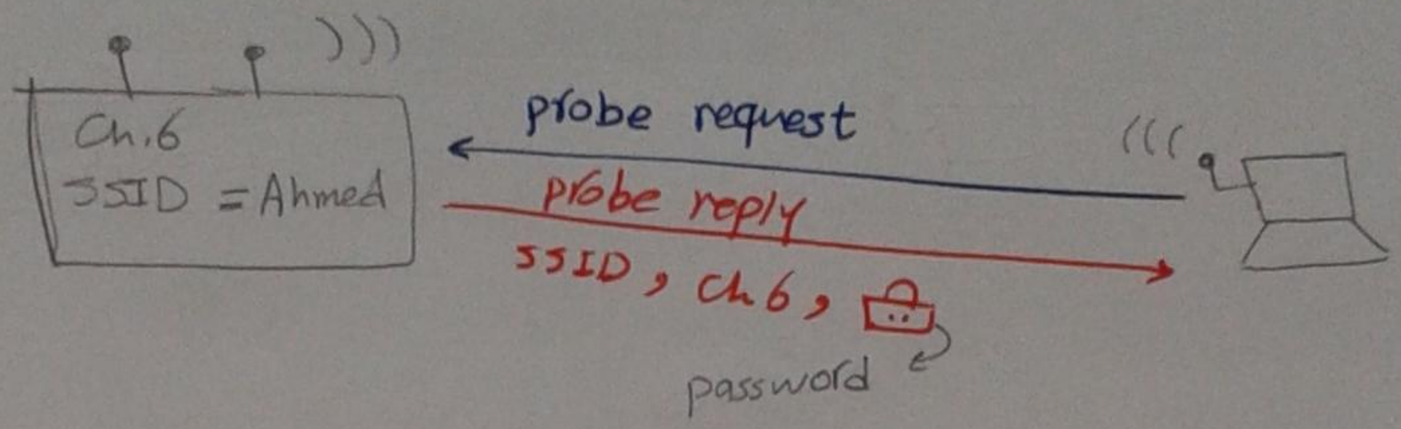




خلصت (الله اكبر)

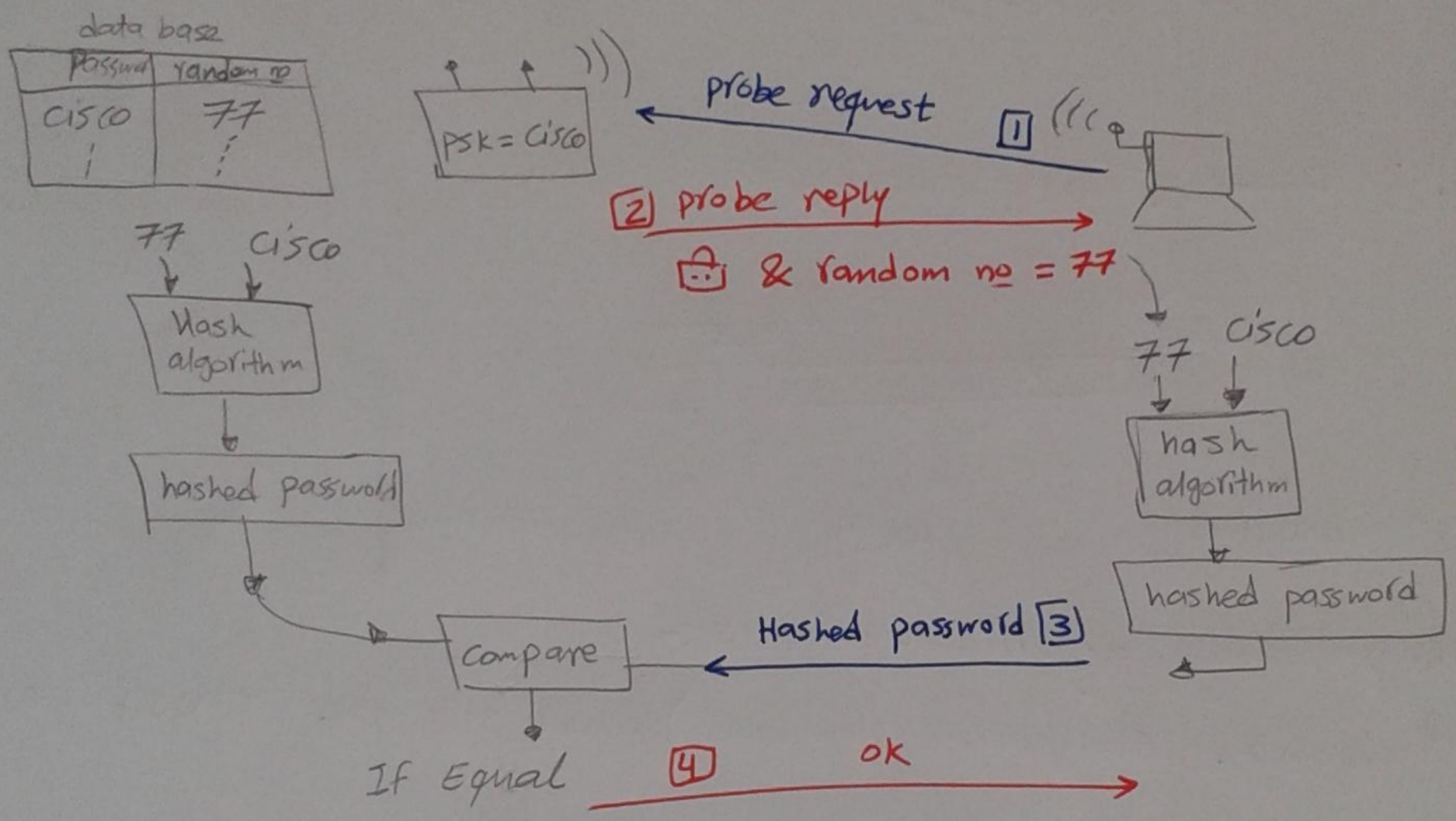
البرنس ⇐ By default بيتغير كل 8 hr وممكن تغييره بالـ Configuration الى 4 hr

wifi security



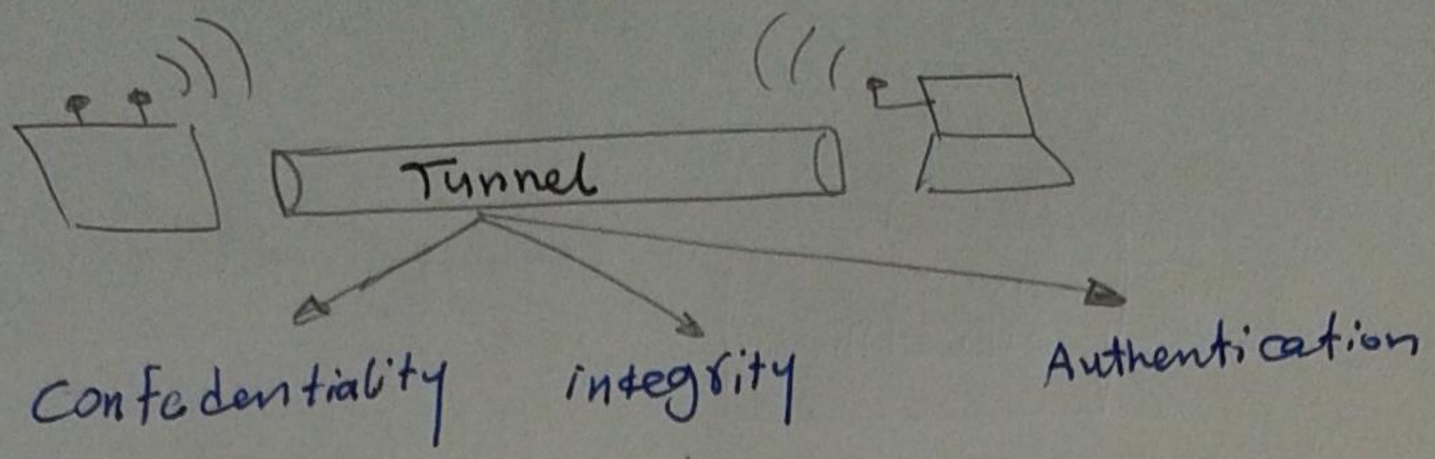
Security types :-

[1] PSK (pre-shared key)



* عيب النوع ده انه اضرب صدر زعالم (weak algorithm)
* اسم الكراك اللى قدر يحل ال algorithm هو air crack ≡ psk crack ≠ WEP crack
  - WEP ← wire less equipment protocol

[2] WPA (wifi protected access)



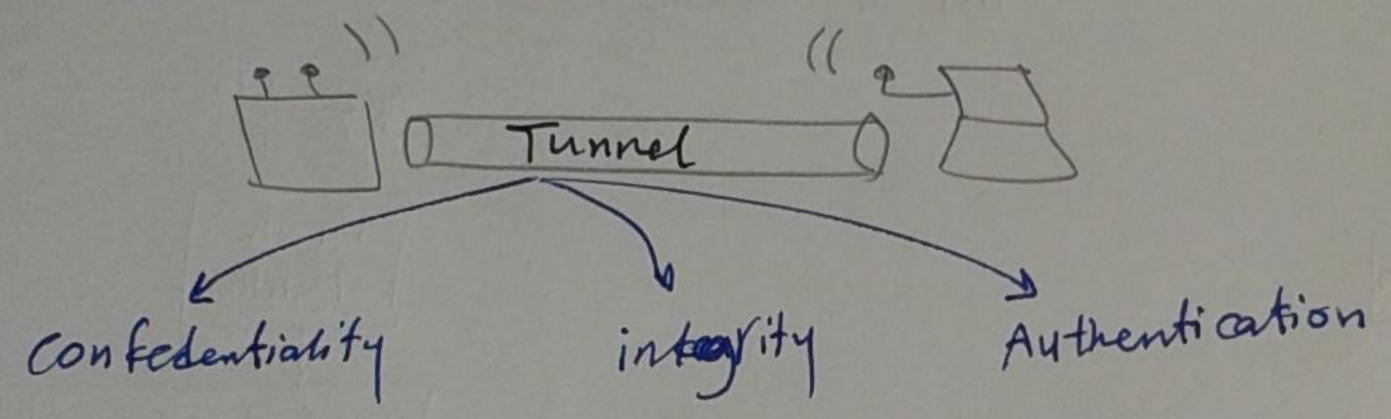
the programs & protocols that used in WAP

① MIC [Message integrity code] is used for integrity process

② TkIp [Temporary key integrity protocol] For confedentiality & Authentication

كنت للاسف اتضرب كنه خد وقت كبير بقبال ما حلوا الـ pass بتاعته

[3] WPA 2 ⟵ الاقوى و متضربش لحد دلوقتى



it is using strong algorithm who is :-

① AES (advanced Encryption Standard), but still use TKIP to backward compatibility with WPA

IPV6

IPV6 is the next Generation Network (NGN)

* تم تطبيقه فى مصر 6/2012

why we need IPV6 ?

we need larger address space

① internet population is increasing

② mobile phones, PC, Notepad, ------

③ Transportation

④ home appliances [smart house]

IPV6 : 128 bit

no of IPs address $= 2^{128} \simeq 3.4 * 10^{38}$ IPV6

$\simeq 5 * 10^{28}$ IPV6/human

Colon ≡ :

* IPV6 is 128 bit represented in Coloned Hexadecimal

note IPV4 is dotted decimal ⟹ 4 octets [one octet = 8 bit]

* IPV6 is 8 Fields

→ each Field is (16 bit ≡ 4 hexadecimal) ∴ IPV6 = 8 * 16 = 128 bit

ex1 203B : 0007 : 00A4 : 0BDF : 0000 : 0000 : 0000 : 0ACD

* IPV6 address rules :-

[1] leading zeros are optional in a feild

203B : 7 : A4 : BDF : 0 : 0 : 0 : ACD

[2] Field of all zeroes = :0:

203B : 7 : A4 : BDF : 0 : 0 : 0 : ACD

[3] fields of successive zeroes = :: ← it is used only once in IPV6

203B : 7 : A4 : BDF :: ACD ← هيتعمل لما كل اللى فى النص اصفار

ex2 203B : 0000 : 0000 : ABCD : 0000 : 0000 : 0000 : 1234

203B :: ABCD :: 1234 → ✗ هيتعمش (::) مرتين فى نفس الـ IPV6 عشانه الـ pc مش هيفهم كام صفر فى الاولى و كام فى التانيه

✓ 203B :: ABCD : 0 : 0 : 0 : 1234 (او) ✓ 203B : 0 : 0 : ABCD :: 1234

EX3 FF02 :0:0:0:0:0:0:0005

⇓

FF02 :: 5 ⟶ المناظر له في IPV4 ⟶ 224.0.0.5

all ospf3 routers

ospf2 with IPV6

all ospf2 routers

* ال ospf اللي اتعلمناه في ال Routing اسمه (ospf2)

EX4 0:0:0:0:0:0:0:1

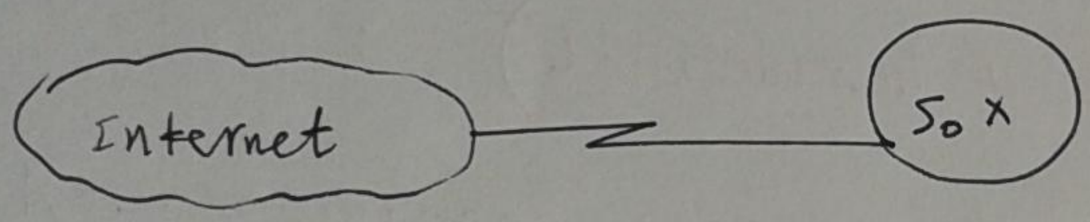
⇓

::1 ⟶ المناظر له في IPV4 ⟶ 127.0.0.1

all IPV6 loopback Icp/IP

loopback ⟹ TCP/IP

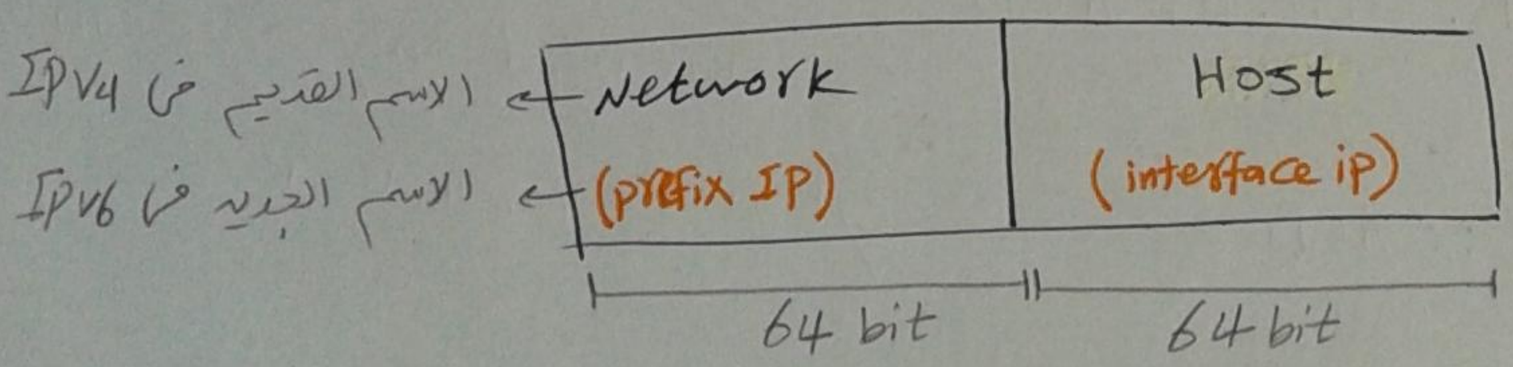
EX5



(config) # ip route 0.0.0.0 0.0.0.0 S0 ⇐ in IPV4

(config) # ipv6 route :: /0 S0 ⇐ in IPV6

IPV6 class is called default class ⇐ there is only one class in IPV6



The default mask /64

How to give IP to DTE ???

1. Statically
2. Dynamically by using DHCPV6
3. Dynamically by using NDP [Neighbor discovery protocol]

---

* NDP operation

Network | host part

IP: 2:0:0:0: - - - - - -

Mask: /64

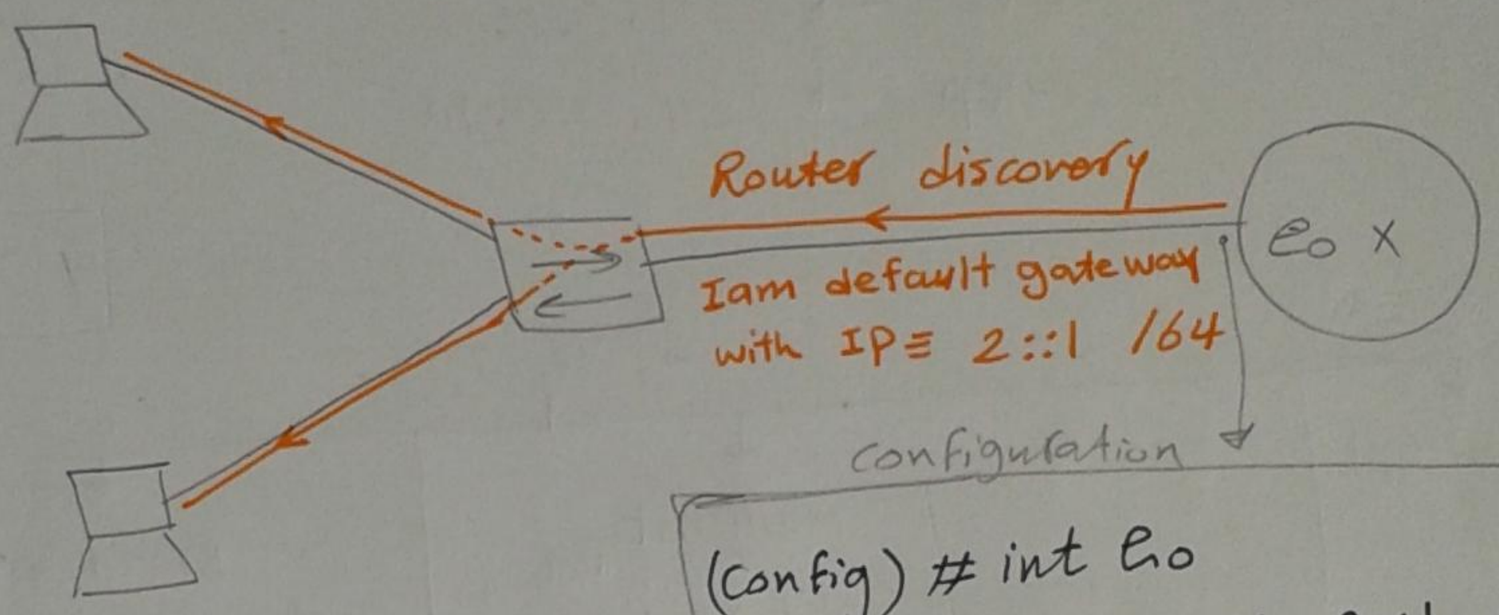
d.g: 2::1

Network | host part

IP: 2:0:0:0: - - - -

Mask: /64

d.g: 2::1



2::1 /64

2:0:0:0:0:0:0:1

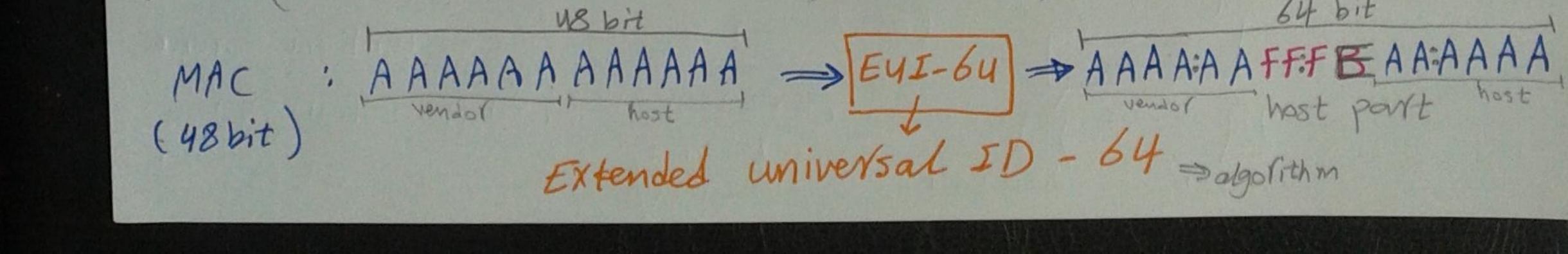
N H

(FF02::2)

* بعد ما ت configure الروتر بالامرين اللى فوق ← هيبعت على ال Broadcast ال (Router discovery) وهيقول فيه [انا ال d.g و ال Ip & Mask 2::1 /64]

* كل pc هياخد ال (Network part) من ال Ip وهيضيفه لنفسه وهياخد ال MAC address بتاعه (48 bit) وهيدخله على protocol اسمه (EUI-64) عشان يضيف 12 bit زيادة لل MAC ويبقى الناتج 64 bit ← ال pc هياخد ال 64 bit دول وهيجعلهم ال host part بتاعه

* ملحوظه ال 12 bit الزيادة هما (FFFE Hexa) ودول ثابتين ومكانهم ثابت



IPV4 types

unicast
Class A
Class B
Class C

Multicast
Class D
224.x.x.x
239.x.x.x

all Routers multicast → 224.0.0.2
all ospf2 → 224.0.05
DR & BDR ospf2 → 224.0.0.6
RIP V2 → 224.0.0.9
EIGRP → 224.0.0.10

Broadcast
255.255.255.255

it is used For protocols as (RIPV1, EIGRP) and application as (DHCP)

IPV6 types

unicast

Multicast
Network | Host
FFXX : ——

all IPV6 Routers ← FF02::2
ospf V3 ← FF02::5, FF02::6
RIP ng (next generation) ← FF02::9
EIGRP For IPV6 ← FF02::A

Broadcast
not supported

فى IPV6 مش هيبقى فى Broadcast ← عشان بيشغل كل الاجهزة فى الشبكة وهيخلى اى حاجه كانت بتشتغل Broadcast ← هيخليها Multicast على ال IP دة FF02::2 يعنى مثلاً ال DHCP هيشتغل Multicast على ال IP دة FF02::2

anycast
- الوضع هنا عشان ازود ال Redundancy & load sharing

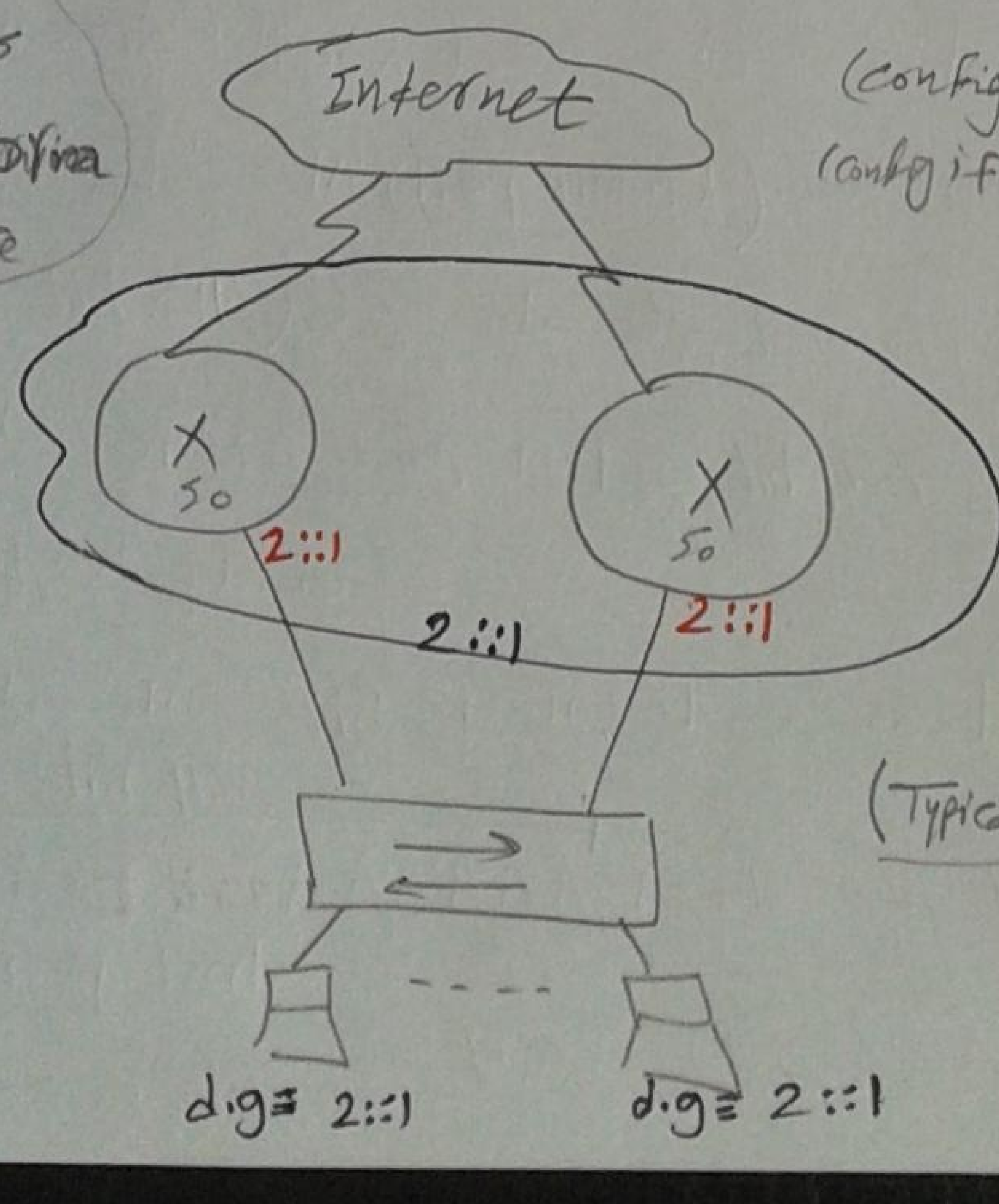
هستخدم 2 Routers متوصلين parallel يعنى بنفس ال LAN من طرف ونفس ال WAN من الطرف التانى

بمعنى، more than one router acts as one big virtual router and give them one big virtual IP

(ليهم نفس ال IP)

العملية دى بيسموها uniform service ← لازم يكون الروترين (يعنى Typical)

the 2 Routers support uniform service



(config)# int S0
(config if)# IPv6 add 2::1 /64 anycast

← انواع ال protocols اللى بتعمل العملية دى
1- HSRP
2- VRRP
→ اتأكد منهم

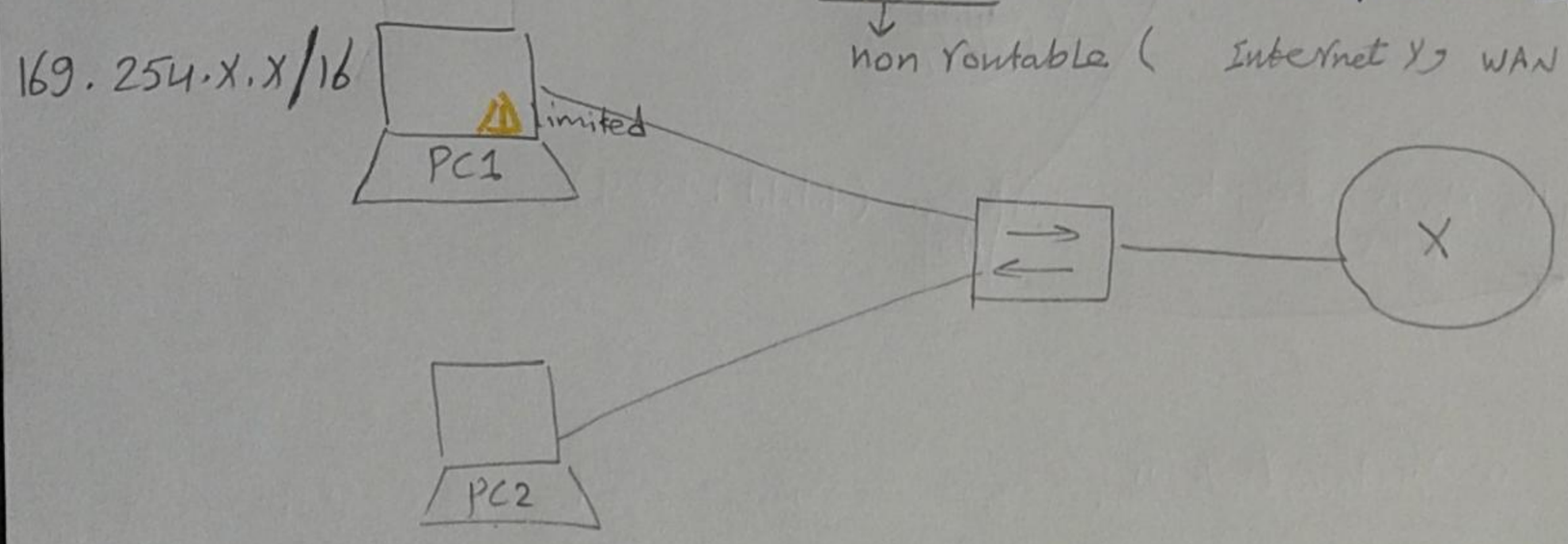
IPV4 unicast

- **loopback**
  - 127.0.0.1
  - مشان تكلم بيها نفسك
  - TCP/IP على ping ← بتاكد
- **private IP in LAN**
  - مشان تكلم بيه اي حد في ال LAN بتاعتك بس
  - Ex
    - manually
    - Automaically
      - DHCP
      - APIPA
- **private IP in LAN / WAN**
  - 10.x.x.x
  - 192.168.x.x
  - 172.16.x.x → 172.31.x.x
- **Real IP (public IP)**

IPV6 unicast

- **loopback**
  - ::1
- **Link local**
  - FE80 : x
  - Ex APIPA
- **site local**
  - FEC0 : x (zero)
- **global**
  - (public IP)
  - لو طالع نت فقط

- Omanually
- O Automatically → DHCP / APIPA (Automatic private IP address)
  - non routable (Internet في WAN على)



لو انت شغال (DHCP) وفي مشكله معينة في الـDHCP server والـ PC1 مش عارف يأخد IP من الـ DHCP server ← اولاً هتظهر علامه صفراء في الـPC وهيقولك فيها limited class

← هنا لازم الـ PC1 ياخد اي IP عشان يشتغل فهيروح واخد اي IP من الرينج ده 169.254.X.X /16

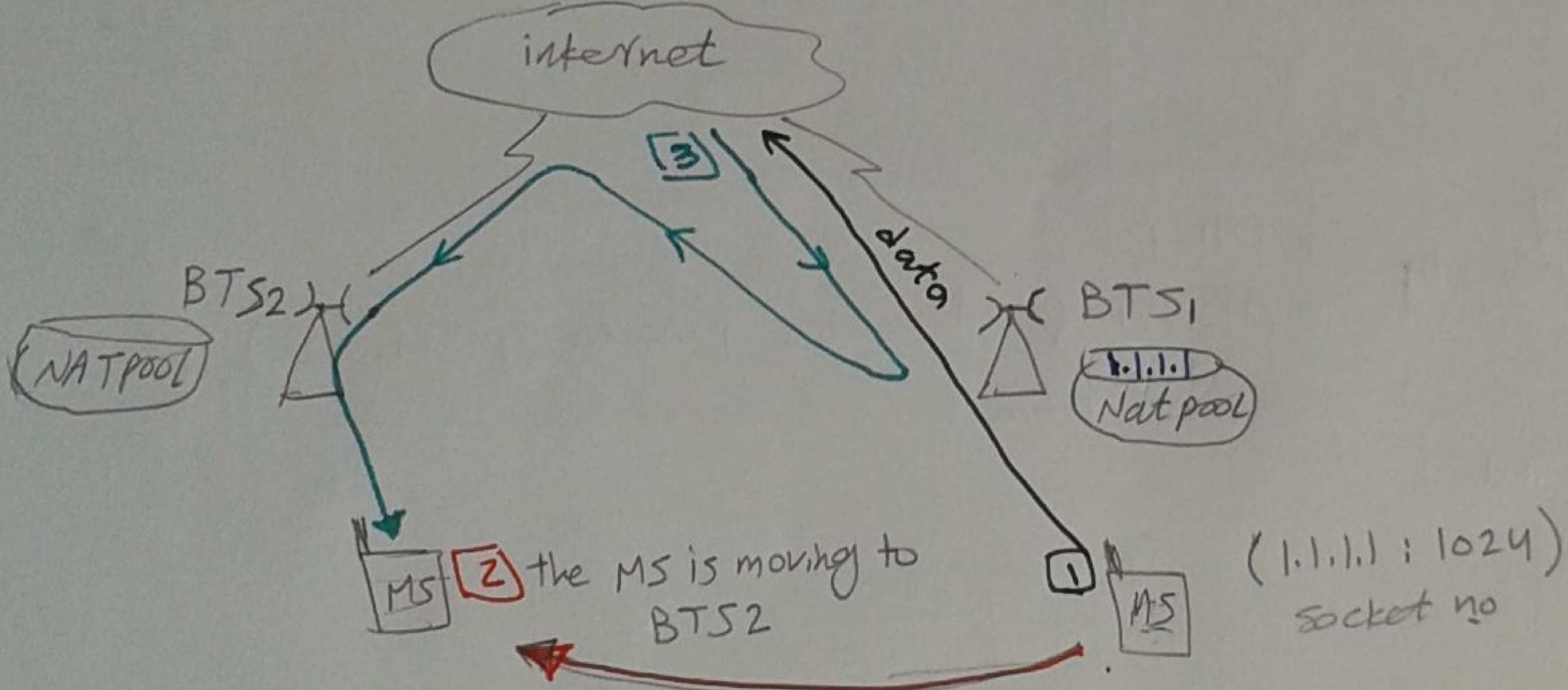
لازم نتأكد الاول انه مفيش حد واخد الـ IP ده قبل كدة

الـ protocol اللي بينفذ العملية دي اسمه APIPA

* IPV6 end to end data delivery

يوجد 7 تحسينات اضافيه في IPV6 عن IPV4

1. Enhancing blug & play configuration (NDP & EUI-64)
2. Enhancing redandundancy & loadshorring (any cast)
3. same routing protocol (RIP ng , ospf3 , static , EIGRP , - - - -)
4. Enhancing Integrated QOS (Buit in header COS)
   class of service ⇒ 8 bit for periority
5. Enhancing integrated security (Built in header IPsec)
   يعني بيتم فيه ⇄ confedintialit / integrity / authentication — زي ال VPN
6. Enhancing Mobility (protocol in header Mobile IP)



لو انت معاك MS وفاتح session معينه في ال Facebook مثلاً ، كده انت معاك socket no
(IP : port) ⇐ لو انت بتتحرك بال MS من BTS1 الى BTS2 ⇐ لو ال IP
اتغير ⇐ ال Data هتقع ، فهنا مينفعش تغير ال socket no بتاعك طالما
مانت فاتح ال session و بالتالى كل ما هتتحرك من BTS1 الى BTS2 ، BTS1
هتقول ل BTS2 خلّى ال IP (1.1.1.1) عندك
⇐ الكلام ده بيتم عن طريق Mobile IP protocol

7 Enhancing integerated advanced switching (Label switching) (Buit in header MPLS)

MPLS : Multiprotocol label switching

الشكله / فى شركات ال service provider لو جت packet ليها IP معين فالروتر
هيقارن ال IP ده بال Routing table اللى عنده عشان يـ Route ال packet
بس المشكلة هنا ان بعض ال Routing table بيكون فيه حوالى 300,000 سطر
وكل الشغل فى الروتر بيكون S/W ⇐ عشان كده العملية دى بتخنق الروترات
اوى وكمان كل ما هتضيف new Technology هتخنق الروترات اكتر
⇐ العملية دى بطيئة جداً فعشان كده الناس فكرت انها تستخدم ال
(label switching) بمعنى هنعمل جدول مناظر ال Routing table بس مفهوش
اى تفاصيل [Mask, protocol...] مجرد علامة لكل IP موجود فى ال Routing table
واول ما ال packet هتيجى، هتروح لل lable switching وهو من غير ما يشوف
اى تفاصيل (يعنى بال label بس) هيوديها لل Next hop router
اللى بينفذ ال lable switching عبارة عن IC (hardware) وده سريع جداً
وبالتالى انا زودت السرعه لـ ١٥ اضعاف على الاقل
اللى بيقوم بالعمليه دى كلها MPLS

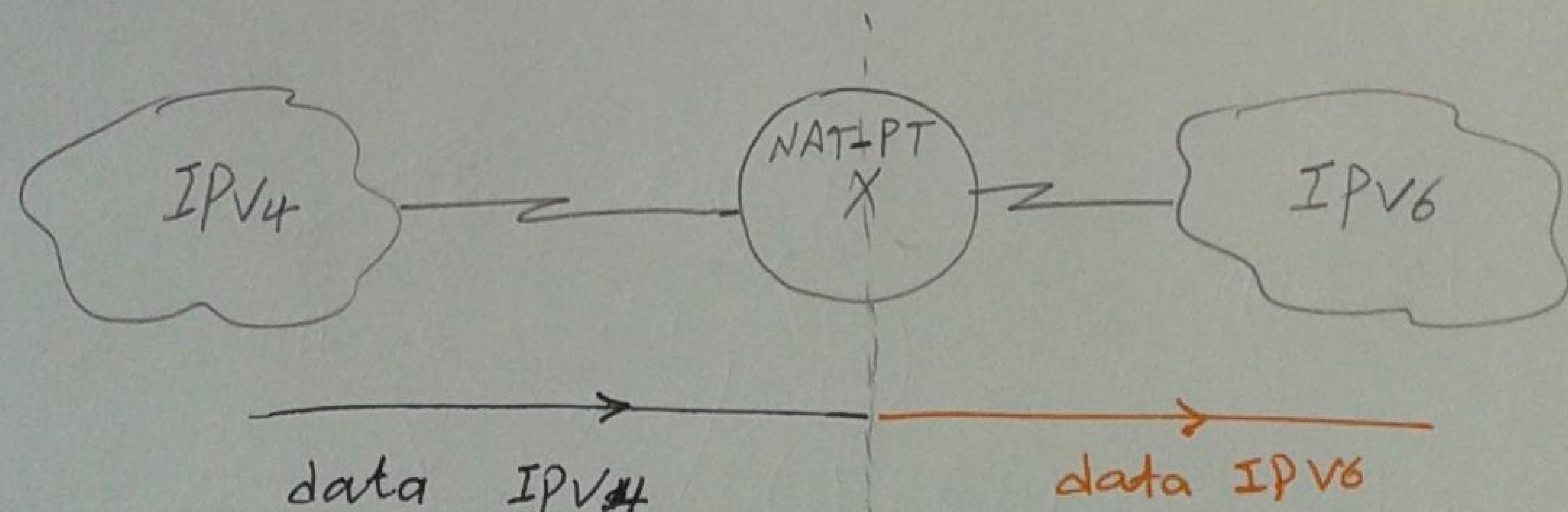
without MPLS ⇒ 10,000 packet/sec
with MPLS ⇒ 10,000,000 packet/sec

---

* IPV4 to IPv6 transition

1. DUAL stack → TCP/IP, TCP/IPv6 — OS (operating system) نازل على TCP/IP & TCP/IPv6

2. NAT-PT (NAT protocol Translation)

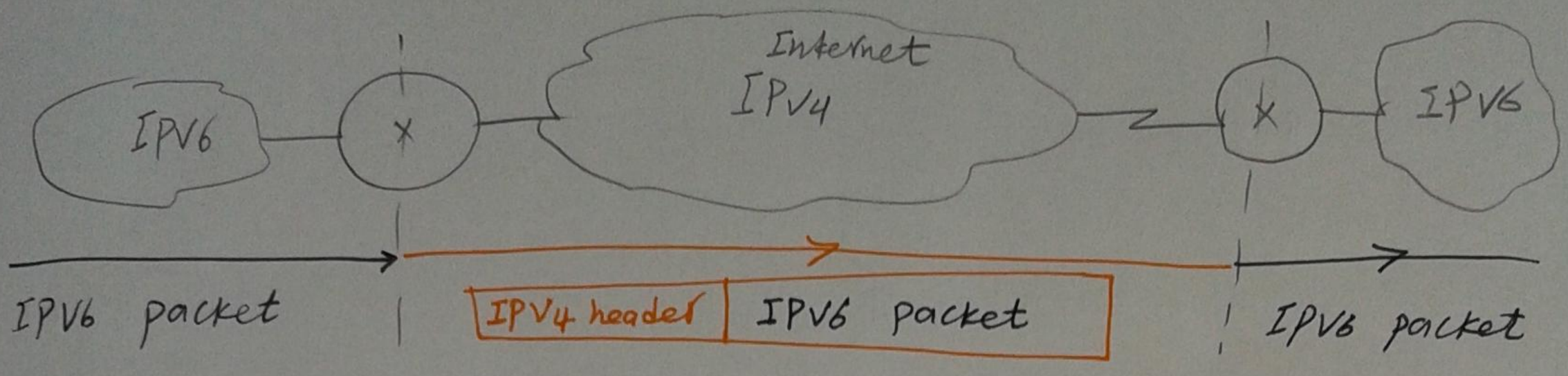


الروتر بيغير شكل ال headers من IPV4 الى IPV6 ⇐ العمليه دى بطيئة ومعقدة شوية

DNS server

IPV6	IPV4
≡	≡

3 Tunneling اختاء

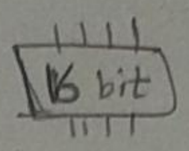


IPV4 فيه header الروتر هيضيف
(address ---)

How to Recover password

Router bootup sequance ↗ load IOS
↘ load configuration file

[1] consult configuration register



By default ← 0X2102 عبارة عن IC (hardwere) 16 bit ، وليها العنوانه دة
↓
Hexa يعني

وشغلتها انها بتستشير الروتر ازى تشغل الـ IOS & configuration

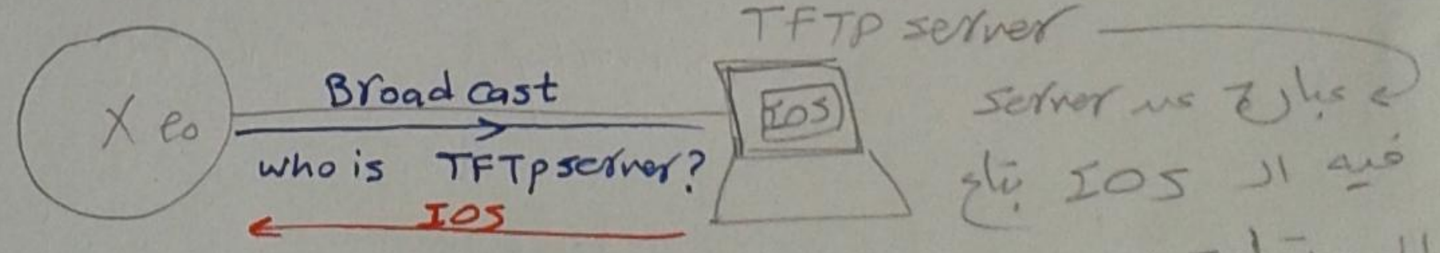
0X2102
العنوانه دة معناه
↙ ↘
load IOS normally — load configiration File normally

[2] load IOS normally

اول لما الروتر بيشتغل بيكونه عايز يـ load الـ IOS

ⓐ Flash
ⓑ TFTb
ⓒ Rommon

فاول حاجه انه هيروح يـ load من الـ Flash
(الـ flash دى هى الـ Harddisc بتاع الروتر)
لو ملقاش الـ IOS فى الـ Flash ← الروتر هيبعت رساله
على الـ Broadcast يقول فيها مين TFTP server
عشانه عايز الـ IOS

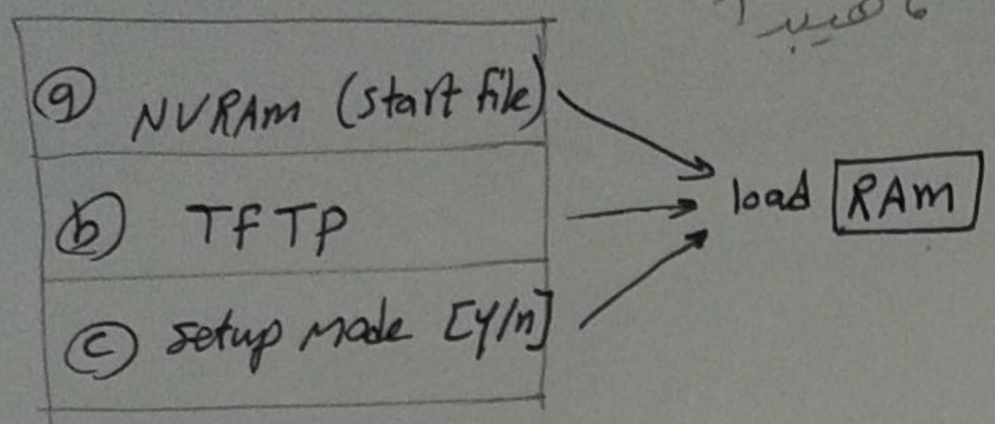


واخر حاجه لو الروتر ملقاش اى TFTp server رد كليه ، هيروح يسأل Rommon
والـ Rommon دة عبارة عن (mini operating sytem)

خلّى بالك من الترتيب عشانه بيجى فى الامتحانه
1- Flash
2- TFTP
3- Rommon

[3] load configuration file (ده فيه الـ password اللي عايز اكسرها)

بعد ما الروتر هيـ load الـ IOS وهيبدأ



يدور على الـ configuration file

اول حاجه هيدور فيها هي الـ NVRAm

← لو لقى الـ Confg. file في الـ NVRAm هيروح يـ load الـ RAM في config. file

← لو ملقاش الـ config file في الـ NVRAm هيروح يدور في الـ TFTP

ولو ملقاش هيروح يدور في الـ setup Mode

password recovery

① اقفل الروتر و بعدين افتحه

② اول ما الروتر يشتغل اضغط على (Ctrl/ Break) عشان الروتر ميكملش تحميل الـ IOS و الـ config. file من الـ Flash والـ NVRAm

← بعد ما تكتب (Ctrl/ Break) هتلاقي نفسك في الـ Rommon

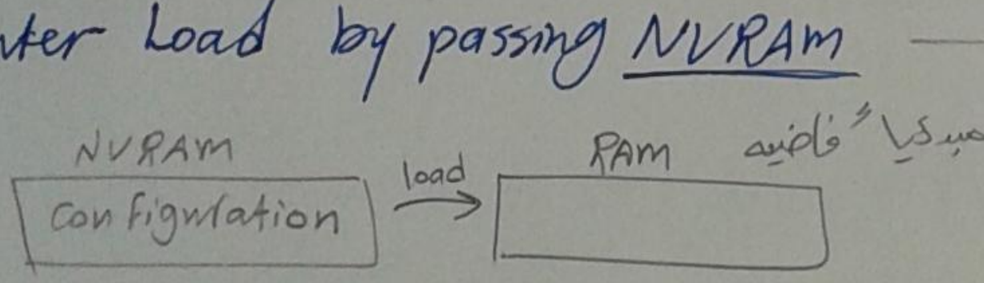
③ Rommon > confreg 0x2143

الرقم ده معناه

- load IOS normaly
- by pass NVRAm (بمعنى مبتبصش على الـ password)

④ router Load by passing NVRAM → آه انت هتدخل على الـ config وهتساوي تلغي الـ passs

(config) # no enable secret
(config) # no enable password



آه انت دولقتي عايز تحمل الـ config من الـ NVRAM الى الـ RAM بالاوامر دة

(config) # copy start run

بعد كده نرجع كل حاجه زي ما كانت عشان نرجع الـ config لـ NVRAm تاني

config-register 0x2102

sh version